

Terry William Ogletree

Firewalls

**Protecția rețelelor
conectate la Internet**

Traducere de Moraru Florin, Mocanu Cristian

Teora

Titlul original: Practical Firewalls

• Copyright © 2001 Teora

Toate drepturile asupra versiunii în limba română aparțin Editurii **Teora**. Reproducerea integrală sau parțială a textului sau a ilustrațiilor din această carte este posibilă numai cu acordul prealabil scris al Editurii **Teora**.

Authorized translation from the English language edition entitled „Practical Firewalls” published by QUE Corporation
Copyright © 2000

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.
Romanian language edition published by Teora Publishing.
Copyright © 2000

Teora

Calea Moșilor nr. 211, sector 2, București
fax: 01/210.38.28
e-mail: teora@teora.kappa.ro

Teora – Cartea prin poștă

CP 79-30, cod 72450 București, România
tel: 01/252.14.31
e-mail: cpp@teora.kappa.ro

Coperta: Gheorghe Popescu

Tehnoredactare: Techno Media

Director Editorial: Diana Rotaru

Președinte: Teodor Răducanu

NOT 4748 CAL FIREWALLS PROTECTIE, REțele
ISBN 973-20-0216-6

Printed in Romania

681.3
376433
BIBLIOTECA
UNIV. TEHNICĂ IAȘI

III-315042

Th

Cuprins

Partea I

Să înțelegem firewall-urile și securitatea în Internet 12

- 1 Elemente de bază despre firewall-uri 13
- 2 Introducere în suita de protocoale TCP/IP 26
- 3 Securitate și Internet 58
- 4 Politici de securitate pentru firewall-uri și strategii de proiectare
a firewall-urilor 75
- 5 Filtrarea pachetelor 95
- 6 Utilizarea unei gazde bastion 112
- 7 Porți de aplicații și servere intermediar 132
- 8 Tehnici de monitorizare și auditare a sistemelor de operare 148

Partea a II-a Criptare și comunicații sigure în Internet ... 165

- 9 Tehnologii de criptare 166
- 10 Rețele virtuale private (VPN) și tuneluri 175
- 11 Utilizarea programului PGP (Pretty Good Privacy)
pentru criptare 188

Partea a III-a Instalarea și configurarea firewall-urilor ... 197

- 12 Instrumente pentru firewall-uri disponibile în Internet 198
- 13 Utilizarea produsului TCP Wrappers 208
- 14 Folosirea setului de instrumente FWTK
(TIS Firewall Toolkit) 217
- 15 SOCKS 241
- 16 SQUID 249
- 17 Utilizarea programelor *ipfwadm* și *ipchains* sub Linux 258
- 18 Microsoft Proxy Server 272
- 19 Firewall-ul Elron CommandView 288
- 20 Dispozitive firewall 299
- 21 Firewall-uri și mai mult decât atât 306

Universitatea Tehnică Iași
BIBLIOTECA

Partea a IV-a Anexe	316
A Porturi uzuale TCP și UDP	317
B Alte instrumente de securitate pe care le puteți folosi.	364
C Resurse suplimentare	372
index	378

Despre autor

Terry Ogletree este consultant și lucrează în prezent în New Jersey. Lucrează în domeniul rețelelor de calculatoare din 1980, începând cu calculatoare PDP și sisteme VAX bazate pe OpenVMS și AlphaServer de la Digital Equipment. Terry lucrează cu UNIX și TCP/IP din 1985 și s-a implicat în problemele legate de Windows NT încă de la apariția acestui sistem de operare. Este autor al lucrărilor *Upgrading and Repairing Networks, Second Edition*, publicată la editura Que, și *Windows NT Server 4.0 Networking*, care reprezintă volumul 4 al seriei *Windows NT 4 Resource Library*, publicată la editura Sams. În plus, a contribuit la realizarea multor alte cărți publicate la editura Macmillan – inclusiv *Windows NT Server Unleashed* (și *Professional Reference Edition*) – și *Special Edition Using UNIX, Third Edition*, publicată la editura Que.

Puteți să îl contactați prin e-mail la adresele ogletree@bellsouth.net sau two@twoinc.com, sau să îi vizitați pagina de prezentare la adresa www.twoinc.com.

Oare ce sunt CRACK și SATAN?	Vezi anexa B, „Alte instrumente de securitate pe care le puteți folosi”, pagina 364
Cum puteți să creați un canal sigur, securizat pentru datele companiei dumneavoastră atunci când este utilizată rețeaua Internet?	Vezi „Ce este o rețea virtuală privată?”, în capitolul 10, pagina 176.
Ce este un atac de tip interzicerea serviciului?	Vezi „Atacuri de tip interzicerea serviciului”, în capitolul 3, pagina 63.
Ce face mai exact un filtru de pachete?	Vezi „Utilizarea unui filtru de pachete”, în capitolul 4, pagina 81.
Învățați de ce aplicațiile intermediar pot fi combinate cu filtrarea pachetelor pentru a crea firewall-uri mai securizate.	Vezi „Strategii pentru firewall-uri”, în capitolul 4, pagina 81.
Nici un firewall nu este perfect. Vreți să știți ce breșe există?	Vezi „Împotriva căror pericole nu vă poate apăra un firewall”, în capitolul 1, pagina 23.
Ce utilitare încorporate de filtrare a pachetelor sunt incluse în sistemul de operare Linux?	Vezi „Ce sunt <i>ipfwadm</i> și <i>ipchains</i> ?” în capitolul 17, pagina 258.
Ce este TIS Internet Firewall Toolkit?	Vezi capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)”, pagina 217.
De unde puteți obține din Internet aplicații gratuite sau shareware pentru a vă construi un firewall propriu?	Vezi capitolul 12, „Instrumente pentru firewall-uri disponibile în Internet”, pagina 198.
Învățați despre configurarea și utilizarea auditării și a fișierelor jurnal.	Vezi capitolul 8, „Tehnici de monitorizare și auditare a sistemelor de operare”, pagina 148
Ce reprezintă programul TCP Wrappers și cum puteți să îl configurați pe un sistem UNIX?	Vezi „Cum funcționează programul TCP Wrappers”, în capitolul 13, pagina 209.
Nu vă place să mâncați SQUID ¹ . Ce rol poate juca însă într-un firewall?	Vezi „Ce este SQUID?”, în capitolul 16, pagina 249.
TCP, UDP, ICMP și protocoalele asociate firewall-urilor sună atât de complicat, însă sunt efectiv ușor de înțeles.	Vezi capitolul 2, „Introducere în suita de protocoale TCP/IP”, pagina 26.
Ați auzit că trebuie să instalați un firewall pentru că firma dumneavoastră primește săptămâna viitoare o conexiune la Internet. Nu aveți nici o idee?	Vezi capitolul 1, „Elemente de bază despre firewall-uri”, pagina 13.
Dacă tocmai ați terminat procesul de înțelegere a versiunii curente de TCP/IP, așteptați până citiți despre IPv6!	Vezi capitolul 21, „Firewall-uri și mai mult decât atât”, pagina 306.
Puteți să instalați și să folosiți software-ul Microsoft Proxy Server pentru a crea un firewall securizat?	Vezi capitolul 18, „Microsoft Proxy Server”, pagina 272.
Vă este teamă să utilizați software descărcat din Internet? Produsele firewall comerciale pot fi ieftine și ușor de instalat, configurat și administrat.	Vezi capitolul 19, „Firewall-ul Elron CommandView”, pagina 288.

¹ În engleză, squid = calmar (n.trad.)

Introducere

În doar câțiva ani, Internetul a început să își facă simțită prezența în toate aspectele vieții cotidiene. În următorii câțiva ani, conexiunile la Internet vor deveni pentru cea mai mare parte a populației la fel de obișnuite ca un telefon. O dată cu această tehnologie aflată în plină dezvoltare s-a creat un domeniu nou, denumit ciber spațiu. Metodele tradiționale utilizate pentru protejarea datelor și a resurselor dintr-o rețea nu vor fi suficiente pentru a asigura securitatea datelor în acest nou domeniu.

Pentru a proteja sigur o rețea conectată la Internet, trebuie să folosiți un firewall¹. Termenul *firewall* poate fi utilizat pentru a denumi o gamă largă de produse proiectate să ajute la protecția rețelei dumneavoastră împotriva amenințărilor externe prin limitarea traficului de rețea care poate să apară între rețeaua proprie și Internet. Cele două tehnologii de bază utilizate pentru a crea sisteme firewall sunt *filtrarea pachetelor (packet filtering)* și *porțile intermediar de aplicație (application proxy gateways)*. Dacă înțelegeți modul de funcționare a acestor tehnologii, vă va fi mai ușor să construiți sau să achiziționați un firewall pentru rețeaua dumneavoastră. În această carte, veți învăța despre ambele tehnologii, ca și despre alte caracteristici importante ale unui firewall, cum ar fi înregistrarea în jurnal, avertizarea și autentificarea.

Cu toate că în prezent există mulți furnizori care vând produse denumite *dispozitive firewall (firewall appliances)*, ar trebui ca înainte să faceți o achiziție importantă să alocăți timpul necesar pentru a înțelege modul în care trebuie construit un firewall și modul în care acesta lucrează. S-ar putea să vi se pară posibil să creați un mediu mai sigur prin construirea unui firewall propriu, folosind un software disponibil prin descărcare din Internet, cum ar fi TIS Internet Firewall Toolkit sau TCP Wrappers, în locul unui produs comercial.

Sunt disponibile puține cărți despre firewall-uri, iar dintre acestea doar câteva au fost editate în ultimul an. Unele încearcă să prezinte toate temele posibile, în timp ce altele fac referire la un anumit produs firewall. În această carte am încercat să prezint cititorului toate conceptele importante folosite pentru crearea firewall-urilor și apoi să arăt cum sunt implementate aceste concepte utilizând produse specifice – atât gratuite, cât și comerciale.

Ce conține această carte?

Conținutul acestei cărți este aranjat pentru a trece de la o introducere simplă la subiecte mai complexe de la un capitol la altul. Dacă sunteți deja familiarizat cu un anumit subiect, veți dori probabil să săriți peste capitolul respectiv. Referințele încrucișate din cadrul textului fac mai ușor de găsit informațiile dacă veți descoperi mai târziu că trebuie să reveniți pentru a înțelege mai bine un concept.

¹ În limba română, firewall a mai fost tradus prin parafoc, perete/zid parafoc/ignifug, zid antifoc, dig/zid de protecție sau chiar zid de foc. Termenul a fost folosit mai ales în domeniul construcțiilor (dar și în aviație) și semnifică un sistem de protecție împotriva incendiilor. În această carte vom folosi termenul original din limba engleză, *firewall*. Termenul va fi explicat detaliat în Capitolul 1. (n.trad.)

Capitolul 1, „Elemente de bază despre firewall-uri”, reprezintă o introducere în domeniul firewall-urilor. Aici veți găsi o analiză referitoare la motivele pentru care ați putea avea nevoie de un firewall și informații despre tipurile de lucruri de care vă poate proteja un firewall și, respectiv, lucruri de care nu vă poate apăra.

Capitolul 2, „Introducere în suita de protocoale TCP/IP”, este dedicat utilizatorilor care nu cunosc încă destul de bine protocoalele TCP/IP și utilitățile asociate acestora în vederea furnizării de servicii de rețea. Dacă ați uitat cum funcționează clasele de adrese sau cum să organizați în subrețele un spațiu de adrese, citiți acest capitol.

În capitolul 3, „Securitate și Internet”, sunt discutate câteva diferențe între modul de implementare a securității într-o rețea simplă și modul cum ar trebui implementată atunci când vă conectați la o rețea mai mare, cum este Internetul. De asemenea, veți găsi aici o prezentare a câtorva metode uzuale folosite de hackeri, cum ar fi atacurile de tip interzicerea serviciului și falsificarea adreselor IP.

În capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, veți găsi informații despre diferitele arhitecturi pe care le puteți folosi pentru a crea un firewall. Aici veți învăța la ce pot servi o zonă DMZ sau o gazdă cu două plăci de rețea și veți găsi o introducere în tehnicile de filtrare a pachetelor și de intermediar de aplicație. Acest capitol vă va permite să luați decizii importante referitoare la modul de creare a unei politici bune de securitate pentru rețeaua dumneavoastră și la modul de implementare a acelei politici cu ajutorul unui firewall.

În capitolul 5, „Filtrarea pachetelor”, este discutat cel mai vechi tip de firewall. Aici veți învăța despre modul în care au fost dezvoltate tehnicile utilizate prima dată pe ruterele cu ecranare pentru a oferi un mecanism care poate să împiedice traficul IP nedorit să treacă prin bariera firewall-ului și să pătrundă în rețeaua dumneavoastră.

Capitolul 6, „Utilizarea unei gazde bastion”, prezintă probleme importante de configurare pe care trebuie să le luați în considerare atunci când selectați calculatoarele care vor fi utilizate pentru a oferi servicii de firewall. Aceste calculatoare sunt cele mai vulnerabile gazde din rețea deoarece sunt expuse în Internet, și din acest motiv trebuie să fie bine configurate pentru a împiedica pătrunderea intrușilor.

În capitolul 7, „Porți de aplicații și servere intermediar”, este analizată o tehnică mai nouă utilizată în firewall-uri. În timp ce un filtru de pachete poate fi folosit pentru a permite sau a interzice fluxul de pachete IP între rețeaua dumneavoastră și exterior, serverele intermediar pot fi utilizate pentru a oferi servicii de rețea fără a permite un flux IP direct între client și server.

Capitolul 8, „Tehnici de monitorizare și auditare a sistemelor de operare”, analizează metode bine cunoscute de configurare a auditării pe sistemele UNIX și Windows NT.

Capitolul 9, „Tehnologii de criptare”, ar trebui citit dacă încă nu înțelegeți conceptele criptografice fundamentale. Aici puteți învăța despre diferențele între tehnicile cu chei secrete și publice și pentru ce este recomandată utilizarea fiecărei metode.

Capitolul 10, „Rețele virtuale private (VPN) și tuneluri”, continuă pe aceeași temă și arată cum pot fi utilizate tehnicile de criptare pentru crearea de conexiuni sigure cu tuneluri printr-o rețea publică, așa cum este Internetul.

Capitolul 11, „Utilizarea programului PGP (Pretty Good Privacy) pentru criptare”, vă poate arăta cum să instalați și să porniți rapid programul PGP pentru nevoile proprii de

securitate, cum ar fi trimiterea de mesaje criptate de poștă electronică semnate cu o semnătură digitală. Tot aici sunt prezentate metodele de instalare pe sistemele UNIX și Windows NT.

Capitolul 12, „Instrumente pentru firewall-uri disponibile în Internet“, vă oferă o privire de ansamblu asupra câtorva dintre cele mai populare instrumente pe care puteți să le descărcați din Internet și, în majoritatea cazurilor, să le folosiți gratuit pentru a construi un firewall.

Capitolul 13, „Utilizarea produsului TCP Wrappers“, detaliază și mai mult modul de instalare și configurare a unuia dintre aceste utilitare gratuite. TCP Wrappers poate fi utilizat pe gazdele UNIX pentru a vă ajuta să securizați accesul la sistem și oferă funcția de înregistrare în jurnal pentru serviciile importante și utile de rețea, cum ar fi Telnet și FTP.

Capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)“, este un alt capitol care prezintă detaliat un produs pe care îl puteți descărca gratuit din Internet. FWTK poate fi dificil de configurat dacă nu sunteți deja familiarizat cu administrarea sistemelor UNIX, însă acest capitol poate reprezenta punctul de plecare în direcția bună, deoarece prezintă concepte importante și vă arată cum funcționează fișierele de configurare.

Capitolul 15, „SOCKS“, prezintă protocolul de securitate SOCKS, care este implementat pe scară largă în produse comerciale, cum ar fi Internet Explorer, și, în plus, este disponibil în bibliotecile care pot fi folosite pentru aplicațiile existente.

În capitolul 16, „SQUID“, este prezentat un alt instrument disponibil gratuit din Internet. SQUID este un server intermediar numai pentru cache care poate fi folosit pentru a furniza controlul accesului, dar și pentru a vă ajuta să gestionați lărgimea de bandă a rețelei memorând copii ale obiectelor Web accesate frecvent într-o memorie cache locală.

Capitolul 17, „Utilizarea programelor *ipfwadm* și *ipchains* sub Linux“, discută despre capabilitățile de filtrare a pachetelor, încorporate în nucleul sistemului Linux, și modul în care cele două utilitare pot fi folosite pentru a administra aceste funcții.

Capitolul 18, „Microsoft Proxy Server“, discută modul de instalare a acestui produs firewall Microsoft. Și aici veți găsi o scurtă introducere referitoare la modul de configurare a serviciilor cu ajutorul interfeței grafice cu utilizatorul proprii serverului.

În capitolul 19, „Firewall-ul Elron CommandView“, este prezentat un alt produs comercial, de data aceasta pentru sistemul Windows NT Server. Sunt analizate modul de instalare și probleme legate de configurarea de bază.

Capitolul 20, „Dispozitive firewall“, analizează o piață nouă pentru firewall-uri, aflată în plină dezvoltare, care încearcă să fie cât mai aproape posibil de tehnologia plug-and-play, sperând să facă procesul de configurare a unui firewall o activitate ușoară pentru utilizatorul final.

În capitolul 21, „Firewall-uri și mai mult decât atât“, veți analiza câteva posibilități pentru noi dezvoltări în domeniul securității în Internet, cum ar fi noua generație a protocolului IP, IPv6. De asemenea, veți găsi aici o discuție referitoare nu numai la protejarea rețelei organizației dumneavoastră, ci și la protejarea calculatoarelor de la domiciliu utilizate pentru accesarea rețelei.

În anexa A, „Porturi uzuale TCP și UDP“, veți găsi o scurtă discuție despre porturile TCP și UDP, împreună cu o listă de porturi general cunoscute și destinațiile acestora.

Anexa B, „Alte instrumente de securitate pe care le puteți folosi“, conține o colecție de instrumente de securitate pe care le veți găsi utile pentru a face calculatoarele din rețeaua dumneavoastră puțin mai sigure. Tot aici veți găsi locațiile de unde puteți descărca utilitare de genul SATAN sau COPS.

În final, în anexa C, „Resurse suplimentare“, este o listă cu surse valoroase pe care le puteți folosi pentru a rămâne permanent la curent cu problemele referitoare la securitatea în Internet și cu tehnologiile pentru firewall-uri. Deoarece amenințările din Internet se modifică rapid, este important să fiți bine informat despre pericolele curente.

Partea I

Să înțelegem firewall-urile și securitatea în Internet

Capitolul 1	• Elemente de bază despre firewall-uri	13
Capitolul 2	• Introducere în suita de protocoale TCP/IP	26
Capitolul 3	• Securitate și Internet	58
Capitolul 4	• Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor	75
Capitolul 5	• Filtrarea pachetelor	95
Capitolul 6	• Utilizarea unei gazde bastion	112
Capitolul 7	• Porți de aplicații și servere intermediar	132
Capitolul 8	• Tehnici de monitorizare și auditare a sistemelor de operare	148

Capitolul 1

Elemente de bază despre firewall-uri

- De ce aveți nevoie de un firewall
- Utilizarea politicii de securitate a sitului dumneavoastră pentru proiectarea firewall-ului
- Tehnologii firewall
- Firewall-uri hardware sau software? Construite sau achiziționate?
- Ce poate face un firewall
- Împotriva căror pericole nu vă poate apăra un firewall

De ce aveți nevoie de un firewall

Atunci când vine momentul să conectați rețeaua companiei la Internet, trebuie să fie luate în considerare mai multe elemente, cum ar fi tipul de conexiune care va fi necesară pentru a asigura o lărgime de bandă suficientă traficului preconizat sau furnizorul ISP. Undeva pe lista dumneavoastră veți include fără nici o îndoială și un rând unde scrie „Fă rost de un firewall“. Este important să înțelegeți că acest element din planul dumneavoastră nu ar trebui considerat o sarcină de rutină, ci ar trebui plasat chiar la începutul listei. Instalarea unui firewall de un anumit tip între rețeaua dumneavoastră și restul rețelelor moderne din lume este una dintre cele mai importante activități pe care va trebui să le efectuați atunci când realizați o conectare la Internet.

Ce este un firewall?

S-ar putea ca până acum cinci ani să nu fi auzit de termenul *firewall*. Înainte de adoptarea acestui termen de către experții în securitate pentru a descrie o metodă de împiedicare a pătrunderii intrușilor nedorți într-o rețea conectată la o rețea mai mare, ați auzit acest termen utilizat în domeniul construcțiilor de clădiri. De exemplu, un firewall poate fi o barieră neinflamabilă între mai multe apartamente dintr-o clădire. Dacă se produce un incendiu într-un apartament, firewall-ul vă poate ajuta să împiedicați focul să se extindă în celelalte apartamente. Ca urmare, firewall-ul ajută la ținerea sub control a problemei.

Când este folosit într-o rețea, un firewall funcționează aproape în același mod: ajută la împiedicarea pătrunderii problemelor din alte rețele în rețeaua locală proprie, fapt care ar putea duce la compromiterea sistemelor și a datelor. Firewall-ul îndeplinește acest obiectiv permițând circulația unui anumit trafic între rețeaua dumneavoastră și Internet și blocând restul de trafic. În timp ce un firewall dintr-o clădire este realizat de obicei dintr-o compoziție simplă din blocuri de ciment sau din alte materiale puternic ignifuge, construcția unui firewall de rețea este mult mai complexă.

Mecanismele utilizate pentru a permite sau a bloca traficul pot fi simple *filtre de pachete* (*packet filters*), care iau decizii în funcție de conținutul antetului de pachet, sau *servere intermediar de aplicație* (*application proxies*¹), mai complexe, care sunt plasate între client și lumea exterioară și acționează ca un intermediar pentru anumite servicii de rețea.

Vezi și

➤ *Ce este un server reprezentant de aplicație? Puteți găsi mai multe detalii despre această tehnică firewall în capitolul 7, „Porți de aplicații și servere intermediar”, la pagina 132.*

Datorită numelui simplu, este ușor să vă gândiți la un firewall ca la un dispozitiv unic sau ca la un singur produs software. Însă în afara celor mai simple cazuri, ar fi probabil mai bine să vă gândiți la un firewall ca la un *sistem*. Este un sistem de componente proiectate să controleze accesul la și din rețeaua dumneavoastră și o rețea externă, pe baza politicilor de securitate valabile în situl propriu. Termenul firewall a fost adoptat pentru a face referire la aceste componente care sunt plasate în general între rețeaua dumneavoastră și lumea exterioară, deoarece firewall-ul pune la dispoziție o barieră, la fel cum un firewall dintr-o clădire oferă o barieră care ajută la prevenirea extinderii focului.

Pe măsură ce între producătorii de firewall-uri a apărut concurența, iar aceștia au încercat să realizeze produse deosebite, au fost dezvoltate caracteristici noi pentru firewall-uri. Deoarece un firewall se găsește la marginea rețelei dumneavoastră și acționează ca un fel de poartă către exterior, este un loc predestinat pentru a efectua o serie de operații care nu au neapărat legătură cu securitatea. De exemplu, între funcțiile noi pe care le puteți găsi într-un firewall modern se numără următoarele:

■ **Lucrul cu memoria cache** Este valabilă în special pentru rețelele care includ servere Web ce oferă informații utilizatorilor din Internet. Prin stocarea locală a datelor accesate frecvent, un server numai pentru cache (caching server) poate să îmbunătățească timpul de răspuns către utilizator și să salveze un procent însemnat din lărgimea de bandă a conexiunii la Internet, care în caz contrar ar fi utilizată pentru aducerea repetată a acelorași date.

■ **Traducerea adreselor** Un firewall configurat corespunzător poate să afișeze în exterior numai propria adresă de rețea, permițându-vă să utilizați orice spațiu de adrese IP pentru rețeaua internă.

¹ proxy = intermediar. Este o componentă a unui firewall și are rolul de a gestiona comunicațiile între o rețea locală și Internet. În lb. română se mai folosește și termenul reprezentant. Autorul folosește aproape interschimbabil în carte expresiile proxy, proxy server, proxy gateway, application proxy, proxy application. (n.trad.)

■ **Restricționarea conținutului** Un număr din ce în ce mai mare de produse vă permit să restricționați tipurile de informații la care le este permis accesul utilizatorilor în Internet, atât prin restricționarea accesului la adrese URL cunoscute ce conțin informații nedorite, cât și prin analiza pachetelor de date primite, după anumite cuvinte cheie.

■ **Vectorizarea adreselor** Această caracteristică permite firewall-ului să modifice anumite cereri, cum ar fi cererile HTTP, și să le trimită către calculatoare gazdă care utilizează o adresă diferită față de cea găsită în pachetul cerere. Astfel, puteți să distribuiți o sarcină de lucru pe mai multe servere, chiar dacă utilizatorilor din Internet li se pare că lucrează cu un singur calculator gazdă.

Aceste caracteristici asigură o serie de avantaje din punctul de vedere al securității, însă în cea mai mare parte a cazurilor ele sunt utilizate pentru a rezolva probleme referitoare la performanță. De exemplu, traducerea și vectorizarea adreselor vă ajută să ascundeți spațiul intern de adrese IP de potențialii hackeri, ceea ce reprezintă în mod clar un beneficiu în favoarea securității. Cu cât sunt mai puține informațiile de care dispune un potențial intrus, cu atât va fi mai grea sarcina acestuia. Însă aceste caracteristici ajută și administratorul rețelei să echilibreze performanțele între mai multe mașini. Utilizarea traducerii adreselor presupune că dumneavoastră nu trebuie să obțineți o subrețea mare de adrese IP care să acopere fiecare stație de lucru și server din rețeaua proprie.

Aici este o adevărată junglă!

Internetul este o lume fascinantă. Însă nu este un loc foarte prietenos. În timp, pe măsură ce sunt dezvoltate standarde și tehnologii noi, aceste lucruri s-ar putea să se schimbe. Însă, la fel ca în toate situațiile în care sunt explorate domenii noi, vor apărea inevitabil probleme cu tehnologia și cu oamenii în timp ce Internetul continuă să crească într-un ritm rapid. Deoarece nu toți oamenii pe care îi veți găsi în Internet vor avea intenții bune, trebuie să țineți cont de elementele de securitate după ce conectați rețeaua proprie la Internet.

Vezi și

➤ *Pentru detalii referitoare la diferitele tipuri de amenințări care au provocat recent probleme în Internet, vezi capitolul 3, „Securitate și Internet”, pagina 58.*

Problemele pe care probabil le-ați întâlnit deja, cum ar fi virușii de calculatoare, vor fi combinate după ce vă conectați la Internet. Acum, în loc să vă îngrijoreze un virus activat de pe o dischetă, trebuie să vă temeți de fișierele atașate la poșta electronică și de programele demonstrative și shareware descărcate din Internet. În loc să vă intereseze să împiedicați angajații să utilizeze sistemul de poșta electronică al companiei pentru a hărțui un alt angajat, trebuie să vă intereseze dacă utilizează în același scop poșta electronică, ce poate ajunge practic oriunde în lume. Dacă ați avut până acum probleme cu stocarea pe stațiile de lucru și pe serverele companiei a unor materiale nedorite, cum ar fi fișiere text cu glume, articole pornografice sau alte materiale similare, așteptați să vedeți ce se întâmplă când vă conectați la Internet!

Utilizarea politicii de securitate a sitului dumneavoastră pentru proiectarea firewall-ului

Înainte să proiectați o strategie de firewall, ar trebui să vă așezați și să vă gândiți la elementele pe care doriți să le protejați și la modul în care doriți să realizați acest obiectiv. Dacă lucrați într-o organizație care nu este o firmă foarte mică, ar trebui să aveți o politică de securitate a companiei respective. Puteți să folosiți această politică pentru a începe. După ce discutați cu utilizatorii dumneavoastră (sau cu șefii acestora), puteți să luați decizii referitoare la tipurile de servicii cărora le veți permite trecerea prin firewall.

Vezi și

- *Veți găsi mai multe informații despre modul în care ar trebui să elaborați o politică de securitate (dacă nu aveți deja una) în capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor” (pagina 75)*
- *Pentru mai multe informații despre serviciile de bază pentru care poate fi utilizată suita de protocoale TCP/IP, vezi capitolul 2, „Introducere în suita de protocoale TCP/IP” (pagina 26).*

După ce analizați aceste servicii și potențialele lor capcane, puteți să decideți care dintre ele sunt necesare în mediul dumneavoastră de lucru.

Amenințări noi împotriva securității care trebuie luate în considerare

Atunci când vă conectați la Internet, deschideți o întreagă lume nouă cu probleme de securitate care vă vor chinui în mod cert dacă nu vă luați măsurile de protecție corespunzătoare. Dacă înainte nu trebuia să vă preocupați decât de greșelile făcute de angajați nepregătiți sau de breșele de securitate create de către un angajat nemulțumit, acum trebuie să vă îngrijoreze fiecare potențial hacker din lume!

La fiecare câteva luni auziți la știrile de noapte o poveste despre un virus nou, un cal troian sau chiar un program de tip vierme care a provocat haos în Internet. Vă gândiți probabil că lumea este plină de programatori foarte inteligenți care pierd luni sau ani de zile în încercarea de a dezvolta un nou program răutăcios sau pentru a pătrunde într-un sit special. Însă, în realitate, aceasta nu este o profesie chiar atât de grea. Multe dintre povestirile de groază pe care le auziți nu se datorează cunoștințelor foarte bune de programare, ci mai ales exploatarea unor erori sau breșe de securitate cunoscute în sistemele de operare sau aplicațiile disponibile în prezent.

Acum câțiva ani, Dan Farmer și Wietse Venema au scris un articol intitulat „Îmbunătățirea securității sitului dumneavoastră prin pătrunderea forțată în el”¹. În acest articol, autorii vă prezintă exemple despre modul în care un hacker poate să folosească utilitare de sistem și programe uzuale pentru a obține informații despre rețeaua dumneavoastră și calculatoarele care fac parte din ea. Ei arată câteva dintre caracteristicile unor programe, cum ar fi

¹ În original, „Improving the Security of Your Site by Breaking Into It” (n.trad.)

sendmail, care au fost exploatate în trecut. Cu toate că unele abuzuri evidențiate în acest articol au fost rezolvate prin utilizarea de petice și programe actualizate, citindu-l vă veți face o idee referitoare la tipurile de lucruri care pot fi realizate și la care dumneavoastră nu v-ați fi gândit niciodată. Cele mai multe dintre sistemele de operare importante utilizate în prezent au fost dezvoltate și folosite inițial pe calculatoare independente sau în rețele mici. Funcțiile de rețea au fost adăugate și îmbunătățite în decursul anilor, dar au rămas încă numeroase caracteristici care nu au fost proiectate pentru mediul interconectat pus la dispoziție de Internet în zilele noastre.

Unde puteți găsi articolul?

Articolul scris de Farmer și Venema, „Improving the Security of Your Site by Breaking Into It”, este disponibil pentru descărcare de pe multe situri diferite din Internet. Dacă utilizați numele autorilor ca intrare pentru un motor de căutare, vă vor fi returnate numeroase locații unde probabil puteți găsi o copie. Este recomandabil ca orice persoană care lucrează într-un domeniu care are legătură cu securitatea rețelelor să citească acest articol.

Hotărâți ce servicii veți oferi utilizatorilor dumneavoastră

De unde ar trebui să începeți atunci când se pune problema creării unei politici bune de securitate pentru rețea? În primul rând, decideți ce tipuri de servicii va trebui să puneți la dispoziție utilizatorilor dumneavoastră. Simplul fapt că stabiliți o conexiune la Internet indică existența unei anumite necesități din partea unui grup de clienți. Care este acea necesitate? Ce componentă a companiei dumneavoastră va beneficia de pe urma rezolvării acestei necesități? Care sunt riscurile pe care le presupune încercarea de a oferi utilizatorilor ceea ce doresc?

Câteva dintre motivele obișnuite pentru care o companie ar dori să se conecteze la Internet sunt următoarele:

- **Poșta electronică** – Pentru a permite angajaților să intre în contact cu furnizorii și clienții.
- **Accesul de la distanță** – Pentru a permite angajaților aflați în deplasare să aibă acces la resursele rețelei LAN locale.
- **Cercetarea** – Pentru a oferi echipei tehnice capabilitatea de a intra în legătură cu colegii de la alte companii și instituții.
- **Asistența tehnică pentru clienți** – Pentru a permite clienților să revadă documentațiile produselor și alte documente în scopul reducerii încărcării echipei tehnice proprii.
- **Asistența tehnică de la furnizori** – Pentru a vă permite dumneavoastră (clientului) să accesați documentațiile și serviciul de asistență tehnică plasate online de furnizorii proprii.
- **Prezența pe piață** – Pentru a realiza afaceri prin comerț electronic și a permite companiei să își prezinte produsele prin Internet.

În funcție de motivele care sunt valabile în cazul dumneavoastră, pot fi utilizate toate sau o parte dintre următoarele tipuri de servicii pentru a oferi utilizatorilor dumneavoastră accesul solicitat:

- **FTP** – Protocolul FTP (File Transfer Protocol) poate fi utilizat de echipa dumneavoastră de cercetare pentru a schimba fișiere de date cu alte situri. Un sit *cu acces FTP anonim* ar putea fi folosit pentru a permite clienților dumneavoastră să aibă acces la fișiere și documentații.
- **Telnet** – Utilizarea acestui serviciu pentru a stabili o sesiune prin conectare de la distanță ar putea fi utilă dacă echipa dumneavoastră de asistență tehnică pentru servicii client trebuie să se conecteze pe calculatorul clientului pentru a diagnostica o problemă. Puteți folosi Telnet pentru a verifica rețeaua de acasă atunci când vă aflați la o conferință sau într-un sit la distanță.
- **World Wide Web (WWW)** – Un server WWW poate oferi companiei dumneavoastră o prezență de piață în Internet. Puteți să țineți clienții la curent cu produsele sau serviciile noi prin utilizarea unui sit Web. Folosind un astfel de sit, pot fi prezentate cu ușurință documentații și servicii de asistență tehnică online.
- **Poșta electronică (e-mail)** – Utilizând protocolul SMTP (Simple Mail Transport Protocol), poșta electronică poate fi livrată de pe calculatorul dumneavoastră de birou aproape oriunde în lume. Poșta electronică poate fi o metodă foarte bună de comunicare rapidă cu clienții și angajații. Dacă luați în considerare costul unui serviciu de poșta actual, nu ar trebui să fie o surpriză dacă în următorii câțiva ani majoritatea firmelor vor începe să trimită facturi prin poșta electronică, pe măsură ce tot mai mulți clienți vor fi conectați.

Vezi și

- *Veți găsi o listă mai mare de servicii în capitolul 2, „Introducere în suita de protocoale TCP/IP”, la pagina 26.*

Aceste servicii de bază nu sunt o listă completă cu serviciile disponibile în Internet. Ele au fost amintite aici pentru ca dumneavoastră să puteți începe să vă gândiți la modul în care doriți să utilizați rețeaua Internet. Când veți avea o listă de servicii care credeți că vor aduce beneficii companiei, trebuie să analizați fiecare serviciu în parte și să răspundeți la câteva întrebări. Există o formă relativ sigură de aplicație client sau server necesară pentru acest serviciu? Modul în care doriți să utilizați serviciul deschide o posibilă breșă de securitate în rețeaua LAN proprie?

Vezi și

- *Deoarece majoritatea serviciilor bazate pe protocoalele TCP și UDP utilizează numere diferite de porturi pentru sesiunile proprii, atunci când vă gândiți la tipurile de servicii pe care doriți să le oferiți utilizatorilor dumneavoastră, consultați și lista de porturi general cunoscute din Anexa A, „Porturi uzuale TCP și UDP”, la pagina 317.*

De exemplu, politica dumneavoastră de securitate ar putea stabili ca utilizatorilor să li se permită să stabilească sesiuni Telnet la distanță, care să treacă prin firewall, însă aceeași politică ar putea stabili să nu fie permisă în nici o situație o sesiune Telnet inițiată de la distanță. Aceasta permite utilizatorilor dumneavoastră să stabilească o sesiune la distanță pe sistemul unui client, însă celor din afară nu le este permis acest lucru în rețeaua dumneavoastră. Puteți să creați politici similare și pentru alte servicii importante de rețea, cum ar fi FTP și SMTP, în funcție de cerințele specifice. La fel ca în cazul oricărui tip de politică, indiferent dacă ține sau nu de securitate, există și excepții.

Vezi și

- *Pentru mai multe informații despre modul în care politica de securitate vă poate ajuta să proiectați un firewall propriu, vezi capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, la pagina 75.*

Politica de firewall

După ce revedeți ce probleme de securitate sunt implicate, puteți să dezvoltați o politică de firewall. Există două metode fundamentale prin care firewall-ul poate fi utilizat pentru a implementa politica:

- Permiteți orice acces, mai puțin cele care au fost interzise în mod specific prin reguli.
- Interziceți orice acces, mai puțin cele care au fost permise în mod specific prin reguli.

A doua strategie este cea pe care ar trebui să o utilizați. De ce? Privind dintr-un punct de vedere logic, este mai ușor să specificați o listă mică cu lucrurile pe care le veți permite decât o listă mai mare cu ceea ce nu veți permite. De asemenea, deoarece în mod frecvent sunt dezvoltate protocoale și servicii noi pe măsură ce rețeaua Internet continuă să crească, nu va trebui să adăugați continuu reguli noi pentru a exclude problemele care vor apărea. Veți rămâne protejat de dezvoltările noi până când veți avea timp să revedeți elementele de securitate și să decideți dacă este cazul să permiteți protocolul sau serviciul respectiv prin firewall.

Vezi și

- *Pentru mai multe informații despre crearea unei politici de firewall, vezi capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, la pagina 75.*

Tehnologii firewall

Există două metode de bază utilizate pentru a crea un firewall de rețea: filtrarea pachetelor și serverele reprezentant de aplicație. Unor administratori le place să includă și alte tehnici, însă de obicei se constată că acestea nu sunt decât simple variații ale celor două metode fundamentale. Fiecare tehnică are propriile avantaje și dezavantaje, astfel că este important să înțelegeți cu exactitate cum operează pentru a vă proteja rețeaua.

Primele firewall-uri: Filtrarea pachetelor

Filtrele de pachete (packet filters) au reprezentat primul tip de firewall dezvoltat pentru a proteja o rețea de Internet. Ruterele erau configurate să permită sau să interzică trecerea pachetelor pe baza unor reguli create de administrator. Deoarece ruterele nu analizau decât informațiile de antet dintr-un pachet IP, erau limitate în ceea ce puteau face. De exemplu, un filtru simplu de pachete putea fi configurat să permită sau să interzică utilizarea protocolului FTP, însă nu putea fi folosit pentru a permite sau a interzice anumite funcții ale protocolului FTP, cum ar fi utilizarea comenzilor GET și PUT.

Vezi și

Pentru a învăța mai multe despre firewall-urile care folosesc filtrarea pachetelor, vezi capitolul 5, „Filtrarea pachetelor”, la pagina 95.

Utilizarea porților de aplicație

Dacă un filtru de pachete nu poate lua decizii decât pe baza informațiilor pe care le găsește în antetul pachetului, pentru a crea un firewall mai complex poate fi utilizat un server reprezentant de aplicație.

Vezi și

➤ Pentru mai multe informații despre servere reprezentant și porți de aplicație, vezi capitolul 7, „Porți de aplicații și servere intermediar”, la pagina 132.

O poartă de aplicație (*application gateway*) sau un server reprezentant de aplicație (*application proxy*) este un program software care rulează pe firewall pentru a intercepta traficul corespunzător unui anumit tip de aplicație. Software-ul reprezentant interceptează cererile utilizatorilor din rețeaua locală, de exemplu, și apoi realizează pentru utilizatorul dumneavoastră o conexiune la serverul care se găsește în afara rețelei LAN a acestuia. Utilizatorul intern nu realizează niciodată o conexiune direct la serviciul extern. Programul reprezentant de aplicație se comportă ca un intermediar și discută cu clientul și cu serverul, schimbând între aceștia informațiile utile aplicației. Avantajul în această schemă este că reprezentantul de aplicație poate fi programat să permită sau să interzică traficul și pe baza informațiilor conținute în secțiunea utilă a pachetului, nu numai pe baza informațiilor din antet. Aceasta înseamnă că reprezentantul de aplicație înțelege metodele fundamentale de comunicație utilizate de un anumit serviciu și poate fi programat pentru a permite sau a interzice funcții ale serviciului, nu doar să blocheze comunicația pe baza portului, așa cum procedează un filtru de pachete.

Alte componente de firewall

Filtrul de pachete și reprezentantul de aplicație sunt metodele de bază utilizate pentru a crea un firewall. Modul în care sunt configurate și dispozitivele întrebuințate reprezintă un subiect mai complex. Gazdele bastion, gazdele de sacrificiu și zona demilitarizată (DMZ, sau demilitarized zone) sunt termeni pe care îi veți auzi în mod frecvent atunci când se discută despre firewall-uri. Mai târziu în această carte, veți analiza cu atenție fiecare dintre aceste tehnici astfel încât să vă puteți decide care dintre ele poate fi utilizată în firewall-ul dumneavoastră.

Vezi și

- Strategiile care utilizează o gazdă bastion sunt discutate mai detaliat în capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, la pagina 75.
- O discuție mai detaliată despre utilizarea unei gazde bastion poate fi găsită în capitolul 6, „Utilizarea unei gazde bastion”, la pagina 112.

Firewall-uri hardware sau software? Construite sau achiziționate?

La început, firewall-urile erau formate în principal dintr-un ruter care era configurat ca un filtru de pachete (acceptând sau refuzând pachetele pe baza informațiilor din antet) și o bază de reguli construită de administratorul de rețea. Pe măsură ce firewall-urile au câștigat mai multe funcționalități, cele mai noi au fost implementate ca programe software care rula pe stații de lucru sau pe servere. Firewall-urile și mai noi sunt create sub forma unor configurații hardware și software ambalate împreună. Aceste cutii hardware noi, denumite uneori *dispozitive firewall* (*firewall appliances*), pot fi formate din aplicații software particulare instalate pe un sistem de operare standard, cum ar fi UNIX, după ce a fost redus la minimumul necesar. Unii producători își proiectează chiar propriile sisteme de operare, știind că hackerii vor cunoaște amănunțit slăbiciunile unui sistem de operare comercial.

Vezi și

➤ Pentru a învăța mai multe despre unele dintre dispozitivele firewall ce se găsesc pe piață și câteva șmecherii pentru evaluarea produselor concurente, vezi capitolul 20, „Dispozitive firewall”, la pagina 299.

Ce tip de firewall ar trebui să utilizați pentru a vă proteja rețeaua de calculatoare? La fel ca în cazul oricărei decizii de achiziție, ar trebui să faceți o alegere bazată pe cerințele de securitate ale rețelei dumneavoastră și pe caracteristicile oferite de firewall. Desigur, ar trebui să analizați dacă bugetul vă permite achiziția firewall-ului (și întreținerea acestuia). S-ar putea ca cerințele formulate de dumneavoastră pentru un firewall să vă permită să obțineți fonduri suplimentare de la cei din conducerea organizației după ce îi convingeți de importanța acestuia.

Dacă dispuneți de o echipă de asistență tehnică pentru rețea cu înaltă calificare, s-ar putea să vă suradă ideea de a crea un firewall propriu, utilizând ruterele și calculatoarele gazdă de care dispuneți. Dacă sunteți într-o firmă mică ce tocmai se conectează la Internet și nu aveți experți proprii, este recomandat să apălați la un producător care vă poate furniza hardware-ul și/sau software-ul și care poate să asigure lucrările de instalare și asistență tehnică necesare.

Hardware sau software? Construit sau achiziționat? Pe măsură ce veți citi restul capitolelor din carte și veți începe să înțelegeți modul în care funcționează diferitele produse firewall, vă veți da seama că sunteți într-o poziție mai bună pentru a pune întrebări și a lua decizii inteligente. Asigurați-vă că implicați în procesul de luare a deciziei utilizatorii sau directorii cheie, care au cunoștințe despre operațiile zilnice care se desfășoară în rețea. Personalul tehnic ar putea cunoaște protocoalele sau aplicațiile care pot provoca apariția unor excepții în politica dumneavoastră de firewall. Prin adunarea de la început a cât mai multe informații, veți ajunge să construiți un firewall mai bun.

Elemente privitoare la sistemul de operare

Un firewall nu trebuie să ruleze pe același tip de sistem pe care îl utilizați pe calculatorul desktop sau pe servere. De exemplu, este posibil să aveți instalat în rețea sistemul Windows NT ca sistem desktop standard pentru utilizatori, și tot Windows NT pentru

serverele de rețea. Aceasta înseamnă că va trebui să utilizați tot Windows NT pe firewall dacă doriți să folosiți reprezentanți de aplicație pentru a permite clienților dumneavoastră să acceseze servicii din Internet? Nu neapărat.

Ar trebui să alegeți un firewall pe baza caracteristicilor pe care le oferă pentru a impune respectarea cerințelor din politica de securitate a rețelei dumneavoastră.

Este important însă ca dumneavoastră să aveți o înțelegere detaliată a modului în care funcționează firewall-ul și să știți cum să îl configurați corect. Aceasta înseamnă de obicei că va trebui să fiți familiarizat cu sistemul de operare folosit de firewall. Dacă nu înțelegeți sistemul de operare, mecanismele sale de securitate și instrumentele utilizate pentru impunerea securității, nu puteți fi sigur niciodată că firewall-ul nu este compromis de cineva care exploatează o slăbiciune (sau caracteristică) a respectivului sistem de operare.

De exemplu, software-ul firewall de care dispuneți s-ar putea să ruleze foarte bine pe un calculator UNIX plasat la marginea rețelei LAN. Verificați fișierele jurnal și sunteți sigur că totul este în regulă și funcționează așa cum trebuie. Însă, deoarece nu înțelegeți protecțiile fișierelor UNIX, nu ați observat că un angajat nemulțumit a făcut ca fișierul de parole să poată fi citit de toată lumea. De asemenea, nu ați observat că angajatul, care ulterior a fost concediat, a fost capabil să acceseze firewall-ul dumneavoastră din Internet și a făcut modificări semnificative în configurația acestuia.

Dacă vă gândiți serios la aceste aspecte, ce ar putea fi mai rău decât să aveți un firewall în care aveți încredere deplină dar nu înțelegeți complet modul în care funcționează? În final, nu ați putea fi sigur cu adevărat că acesta lucrează așa cum ar trebui.

Vezi și

➤ *Veți găsi un studiu detaliat privitor la problemele de securitate din sistemele de operare UNIX, Linux și Windows NT în capitolul 8, „Tehnici de monitorizare și auditare a sistemelor de operare”, la pagina 148.*

S-ar putea să vă fie teamă să utilizați sistemele Windows NT, UNIX, Linux sau chiar un alt sistem de operare, pe baza știrilor pe care le auziți regulat despre o nouă eroare de programare sau despre o problemă nouă care circulă în Internet. În ultimii câțiva ani, mulți au criticat sistemul Windows NT, spunând că platforma nu este suficient de stabilă pentru a fi utilizată într-un mediu cu nivel ridicat de securitate. Însă dacă aveți timp să studiați, veți descoperi că toate sistemele de operare au propriile puncte slabe. Noile versiuni de Windows NT vor conține în mod sigur probleme care vor trebui rezolvate de producător. Nici noile versiuni de UNIX și Linux nu vor fi perfecte. Cu cât este folosit pe scară mai largă un sistem de operare, cu atât vor fi mai expuse punctele slabe.

Important este însă faptul că în spatele produsului se găsește un furnizor responsabil care poate să monitorizeze descoperirea acestor tipuri de probleme și să le remedieze repede. Dacă sunteți sigur că stăpâniți bine sistemul de operare utilizat de soluția de firewall pe care ați ales-o, chiar nu contează dacă este același sistem de operare utilizat pe calculatoarele desktop sau pe serverele din restul rețelei. În numeroase cazuri întâlnite în prezent, rețelele nu mai sunt omogene, ci reprezintă un conglomerat de mai multe tipuri de sisteme de calculatoare și de protocoale de rețea.

Ce poate face un firewall

Un firewall nu poate face chiar orice pentru a vă proteja rețeaua de calculatoare și nu ar trebui considerat o soluție unică pentru toate problemele dumneavoastră de securitate. Este important să înțelegeți modul în care un firewall vă protejează în realitate rețeaua. De asemenea, este la fel de important să înțelegeți de ce amenințări nu vă poate apăra un firewall. În general, avantajele pe care le puteți aștepta de la un firewall bine construit sunt următoarele:

- Vă protejează împotriva protocoalelor și serviciilor nesigure.
- Protejează informațiile despre utilizatori, sisteme, adrese de rețea și aplicațiile care rulează în rețeaua dumneavoastră de persoanele curioase din afara rețelei.
- Pune la dispoziție evidențe de auditare (prin fișiere jurnal) care conțin date statistice și de securitate ce pot fi utilizate pentru a vă asigura că rețeaua dumneavoastră este sigură și operează eficient. De asemenea, un firewall bun vă permite să configurați avertizări astfel încât să fiți atenționat despre evenimentele semnificative, cum ar fi o tentativă de pătrundere forțată în rețea.
- Pune la dispoziție o gestiune centralizată a securității rețelei față de lumea exterioară. Pentru rețeaua dumneavoastră, firewall-ul este poarta către Internet. Într-o rețea mare, s-ar putea să aveți mai multe conexiuni către rețelele din exterior și, ca urmare, mai multe firewall-uri. Într-un astfel de caz, ar trebui să vă asigurați că ați analizat cu atenție produsele concurente. Numeroase produse mai noi vă permit să administrați mai multe instalări de firewall-uri de la aceeași consolă de comandă.

Ce este traducerea adreselor de rețea?

O altă caracteristică a unor tipuri de firewall-uri, ce devine foarte utilă pe măsură ce domeniul de adrese Internet se epuizează, este *traducerea adreselor de rețea* (*network address translation*, sau NAT). Tehnologia NAT oferă o serie de avantaje de securitate prin ascunderea adresei reale de rețea a unui calculator gazdă atunci când acel calculator face cereri către servere din Internet. Un firewall ce utilizează NAT realizează această funcție prin utilizarea propriei adrese de rețea în locul adresei clientului atunci când trimite cereri către servere din Internet. Atunci când sosesc răspunsurile la cereri în componenta NAT, firewall-ul plasează adresa reală a clientului în pachet și trimite răspunsul mai departe la client. Prin utilizarea funcției NAT, ar trebui să devină evident faptul că nu aveți nevoie decât de o singură adresă pentru a vă conecta rețeaua LAN proprie la Internet.

Împotriva căror pericole nu vă poate apăra un firewall

Un firewall nu vă poate apăra de amenințările din interiorul rețelei. Astfel, dacă aveți un utilizator care este hotărât să provoace dezordine în rețeaua dumneavoastră, trebuie să vă protejați prin folosirea securității de la nivelul calculatoarelor gazdă. Un element foarte important pe care trebuie să îl luați în seamă atunci când utilizați un firewall este că acesta nu poate avea grijă prin nici un fel de vrăjitorie de toate problemele de securitate care pot exista în rețeaua dumneavoastră. *Un firewall nu înlocuiește măsurile zilnice de securitate și de gestionare a sistemului.* Un firewall nu este decât un alt nivel de securitate.

Indiferent cât de sigur ați putea crede că este firewall-ul dumneavoastră, nu trebuie să slăbiți securitatea de la nivelul calculatoarelor gazdă. De fapt, chiar este adevărat contrariul.

Atunci când vă conectați la Internet, indiferent cât de sigur ar fi firewall-ul dumneavoastră, ar trebui să fiți mai vigilent în monitorizarea mecanismelor de securitate ale stațiilor de lucru și ale serverelor din rețeaua LAN proprie astfel încât să vă puteți asigura că nu apar breșe de securitate.

Între pericolele de care nu vă poate proteja un firewall se numără următoarele:

- **Virusii** – Cu toate că anumite produse firewall oferă asistență tehnică pentru detectarea virusilor în traficul care străbate firewall-ul, sunt prea multe metode prin care un hacker inteligent poate să împacheteze un software virus. Chiar dacă firewall-ul pretinde că efectuează o scanare pentru virusi, nu dezactivați software-ul de detectare a virusilor care rulează pe calculatoarele individuale din rețeaua dumneavoastră!
- **Caii troieni** – Similar cu amenințarea virusilor, este dificil să împiedicați programele de tip cal troian să pătrundă într-o rețea. Este ușor de păcălit un utilizator și de a-l face să descarce un program sau să deschidă un fișier atașat la un mesaj de poștă electronică, prin care să se permită rularea unui cod răufăcător pe sistemul local.
- **Social engineering** – Acest termen a devenit cunoscut în ultimii câțiva ani și descrie metodele pe care hackerii le folosesc pentru a obține informații de la utilizatorii „prietenoși”. S-ar putea să fiți surprins să aflați câte persoane își dezvăluie parola atunci când cineva le telefonează și se recomandă a fi un ofițer de securitate care „verifică” ceva. Un firewall nu poate să oprească un angajat slobod la gură.
- **Întreruperile fizice** – Un firewall nu vă poate apăra în cazul unei întreruperi în alimentarea cu curent sau al unei întreruperi într-un cablu de rețea sau telefonic. Precauțiile împotriva acestui tip de eveniment ar trebui să constituie subiectul unui plan de recuperare a rețelei în caz de dezastru.
- **Incompetența** – Angajații slab pregătiți sau un stil neglijent de conducere pot conduce la probleme de configurare, atât în rețeaua LAN locală, cât și în firewall. Dacă angajații nu înțeleg modul în care funcționează un firewall și modul corect de configurare a acestuia, veți avea probleme.
- **Atacurile din interior** – Un firewall nu poate opri o persoană care se găsește deja în rețeaua dumneavoastră să vă facă probleme. Este unul din motivele pentru care securitatea calculatoarelor gazdă rămâne importantă și după ce ați instalat un firewall.

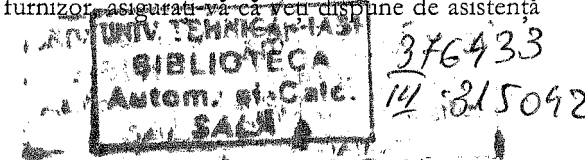
Întreținerea unui firewall

Un firewall nu este un produs pe care doar îl cumpărați, îl configurați și apoi uitați de el. Datorită faptului că natura amenințărilor potențiale care vă pot invada rețeaua se schimbă constant pe măsură ce Internetul se mărește și sunt dezvoltate noi servicii și aplicații, trebuie să fiți vigilent. Indiferent dacă vreți să construiți un firewall pornind de la zero, dacă îl realizați din componente cumpărate de la diferiți producători sau decideți să achiziționați un sistem firewall complet de la un singur furnizor, sunt câteva lucruri la care ar trebui să vă gândiți. Aceste elemente au legătură cu utilizarea și întreținerea firewall-ului în timp. Iată câteva dintre ele:

- **Documentația** – Este necesară o documentație bună dacă vreți să vă familiarizați cu modul în care funcționează componentele firewall-ului. În timpul eforturilor de depanare, un set bun de documentație este o necesitate absolută.

- **Un serviciu bun de asistență tehnică pentru client** – Dacă achiziționați un produs de tip firewall de la un furnizor, nu uitați să îi puneți câteva întrebări despre trecutul companiei și politicile de asistență tehnică pentru clienți. Indiferent cât de bună este documentația, este sigur că într-o zi va apărea o întrebare sau o problemă la care veți avea nevoie de ajutor. Aflați dacă asistența tehnică este disponibilă online sau prin telefon, câte ore pe zi și, ceea ce este și mai important, cât costă.
- **Interfață cu utilizatorul simplă și intuitivă** – Dacă produsul este dificil de gestionat, va fi supus la greșeli de administrare. O bună interfață grafică cu utilizatorul sau o interfață în linie de comandă bine construită pot ușura sarcinile de gestionare zilnice.
- **Actualizările software-ului** – Oferă furnizorul actualizări ale produsului la intervale regulate? Care este costul? Sunt disponibile actualizările pe măsură ce sunt descoperite noi erori de programare în sistemele de operare sau în aplicații?
- **Instruirea** – Oferă furnizorul instruire pentru produs? Este disponibilă în compania dumneavoastră sau este necesară deplasarea? Este posibilă instruirea online sau bazată pe calculator? Și, din nou, cât costă?

Orice aplicație software sau componentă hardware de calculator pe care o achiziționați trebuie să fie însoțită de un serviciu bun de asistență tehnică dacă va fi utilizată într-un mediu de afaceri. Acasă ați putea să trăiți o săptămână, cât timp calculatorul se găsește la magazin. La birou, o rețea sau un calculator dezafectat poate disponibiliza temporar mai multe persoane și poate aduce prejudicii financiare companiei respective. Din această perspectivă, un firewall nu se deosebește cu nimic de alte aplicații critice pentru afaceri. Dacă acordați chiar dumneavoastră asistență tehnică pentru firewall, asigurați-vă că echipa de care dispuneți are abilitățile tehnice necesare pentru gestionarea și actualizarea firewall-ului. Dacă achiziționați un produs de la un furnizor, asigurați-vă că veți dispune de asistență tehnică atunci când veți avea nevoie.



Rezumat

Un firewall este o necesitate dacă doriți să conectați rețeaua LAN proprie la Internet. Firewall-urile pot analiza traficul care intră și iese din rețeaua dumneavoastră LAN și iau decizii în privința tipurilor de trafic pe care le permit sau le interzic. Tehnicile de genul filtrarea pachetelor iau decizii pe baza informațiilor ce se găsesc în antetul pachetului de rețea, cum ar fi adresa pachetului sau protocolul de rețea utilizat. Reprezentanții de aplicație acționează ca intermediari și interacționează cu serverele din Internet astfel încât clienții din rețeaua LAN internă să nu fie expuși comunicării directe și, astfel, unui potențial abuz.

Pentru a decide ce tip de firewall veți construi sau veți cumpăra, inițial trebuie să analizați politicile de securitate curente și să evaluați serviciile pe care utilizatorii se așteaptă să le primească după conectarea la Internet. Utilizând politica de securitate, puteți să proiectați o strategie de firewall folosind rutere, gazde bastion și alte tehnici în scopul protejării rețelei proprii.

În capitolul următor, veți analiza suita de protocoale TCP/IP și alte protocoale care au legătură cu acestea și care sunt utilizate pentru a oferi servicii de rețea în Internet. După ce veți înțelege această tehnologie, veți trece la capitolul 3, care analizează câteva probleme și capcane de securitate asociate unei conexiuni la Internet.

Introducere în suita de protocoale TCP/IP

- Ce este TCP/IP?
- Modelul de rețea OSI
- Protocoalele TCP/IP
- Adresarea IP
- Analiza conținutului unei datagrame IP
- Ce sunt porturile TCP și UDP?
- Servicii TCP/IP uzuale
- Alte servicii de rețea

Ce este TCP/IP?

TCP/IP este prescurtarea de la Transmission Control Protocol/Internet Protocol. Acestea sunt principalele protocoale de rețea utilizate în Internet pentru transferul datelor dintr-un loc în altul. Pe lângă aceste două protocoale importante, mai există multe alte protocoale și utilitare care au legătură cu ele și care de obicei sunt grupate împreună și sunt denumite TCP/IP Protocol Suite (Suita de protocoale TCP/IP). Această suită de protocoale include elemente cum ar fi protocolul de rezolvare a adreselor (Address Resolution Protocol, sau ARP) și protocolul pentru datagramele utilizatorilor (User Datagram Protocol, sau UDP). Utilizatorii finali s-ar putea să nu recunoască acești termeni, însă au auzit probabil de Telnet și de protocolul de transfer al fișierelor (FTP, sau File Transfer Protocol).

Una dintre activitățile pe care trebuie să le efectuați atunci când configurați un firewall este luarea deciziei în ceea ce privește protocoalele și serviciile care ar trebui permise pentru utilizare între rețeaua dumneavoastră și Internet. Unele sunt în mod inerent mai periculoase decât altele și trebuie să fie analizate astfel încât să puteți înțelege riscul asociat cu folosirea lor. Nu uitați regula de aur a unui firewall: Interziceți totul și apoi permiteți doar ceea ce aveți nevoie.

Stive de protocoale și suite de protocoale

Când se discută despre protocoale, termenii *stivă de protocoale* și *suită de protocoale* sunt utilizați deseori cu aceeași semnificație. Acești termeni sunt folosiți pentru a indica faptul că, de obicei, nu este utilizat un singur protocol pentru

comunicație, ci există mai multe protocoale aflate în legătură. Astfel, când discutați despre comunicații în Internet, discutați despre suita (sau stiva) de protocoale TCP/IP deoarece protocoalele utilizate, între care se numără TCP, IP, UDP, ARP și SMTP, execută funcții diferite, dar au fost proiectate să lucreze împreună.

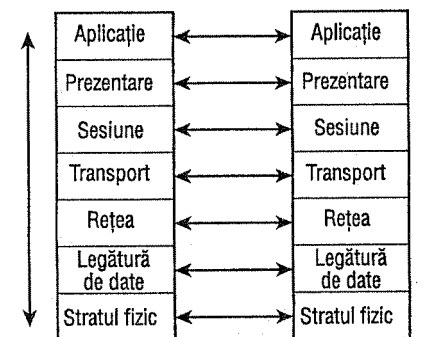
De exemplu, atât TCP cât și UDP folosesc IP pentru funcțiile de adresare și pentru transferul datelor în Internet. Protocolul IP nu poate să efectueze singur această activitate. IP folosește protocolul ICMP pentru funcțiile de gestionare și raportare a erorilor. Mai jos în stiva de protocoale veți găsi protocolul de rezolvare a adreselor (Address Resolution Protocol, sau ARP), care este responsabil pentru determinarea adresei hardware reale a unui calculator, asociată cu adresa IP.

Modelul de rețea OSI

Dacă ați lucrat vreodată ca programator, vă veți aminti de termeni cum ar fi „programare structurată” sau „programare de sus în jos”, precum și de mulți alți termeni utilizați pentru a descrie metodele standard folosite pentru proiectarea și scrierea codului pentru o aplicație. Repartizarea funcțiilor specifice ale programului în componente modulare poate ușura modificarea și întreținerea programului. În 1984, organizația internațională de standardizare (International Standardization Organization, sau ISO) a dezvoltat un model destinat să ajute la standardizarea modului în care erau implementate protocoalele de rețea astfel încât funcțiile specifice să poată fi izolate în componente care puteau fi întreținute cu ușurință. A rezultat modelul de rețea OSI (Open Systems Interconnection). Organizația ISO a utilizat acest model pentru a dezvolta un set de protocoale de rețea deschise, însă acestea nu au fost adoptate niciodată pe scară largă. Oricum, modelul de rețea OSI este încă utilizat atunci când se discută de protocoale de rețea și este recomandat să vă familiarizați cu el dacă veți lucra în acest domeniu. Figura 2.1 prezintă, din punct de vedere conceptual, modul în care se dorește să opereze modelul.

FIGURA 2.1

Modelul OSI este format din șapte straturi care oferă servicii straturilor vecine.



Fiecare *strat (nivel)* din model oferă servicii straturilor adiacente. Aceasta înseamnă că fluxul real de informații începe de la stratul situat cel mai sus în ierarhie, stratul aplicație, care apelează la serviciile oferite de stratul prezintăre, care folosește serviciile furnizate de stratul sesiune și așa mai departe. Cel mai jos în ierarhie este situată componenta fizică a rețelei. La acest nivel este definit modul în care sunt transmise datele prin rețea – de la cablare până la plăcile de rețea și la conectoarele utilizate prin canalul fizic.

Când ajung la un alt nod pe stratul fizic, datele încep să urce prin celelalte straturi; software-ul de pe fiecare strat utilizează funcții ale stratului superior până când, în final, informațiile ajung la stratul aplicație, unde pot fi în legătură cu utilizatorul.

Acesta este fluxul *fizic* al informațiilor prin model. Privind dintr-o perspectivă *logică*, fiecare strat din model comunică cu stratul corespondent din nodul situat la distanță. De exemplu, software-ul de pe stratul aplicație nu este interesat decât de modul de comunicare cu stratul aplicație din nodul situat la distanță. Software-ul scris pentru acest nivel nu trebuie să înțeleagă modul în care ajung datele la stratul aplicație corespondent de la celălalt capăt al conexiunii. Nu contează dacă datele circulă pe cabluri de fibră optică sau pe conexiuni 10BASE-T – cel puțin atunci când este implicat stratul aplicație. Invers, componentele care lucrează la nivel fizic nu sunt interesate dacă informațiile trimise sau recepționate sunt texte ASCII sau date codate binar. Stratul fizic este preocupat numai de lucrul cu stratul fizic din nodul situat la distanță pentru a trimite și a prelua datele la/de la sistemul acestuia.

Stratul fizic

La acest nivel este realizat procesul fizic de mutare a biților de date printr-un mediu de rețea. Componentele rețelei definite la acest nivel sunt:

- Cablarea
- Conectoarele
- Tehnicile de semnalizare (electrice și optice)

Acest strat este probabil cel mai ușor de clasificat. Este format din toate componentele fizice ale rețelei care sunt implicate în trimiterea și recepționarea biților de informații. Aici este definit numărul de pini ai unui conector; de asemenea, la acest nivel este definit modul de interpretare a unui semnal (de exemplu, codarea Manchester și Manchester diferențială).

Cum puteți să rețineți straturile din modelul de rețea OSI?

Dacă vă pregătiți să susțineți un test de certificare și vă dați seama că aveți o problemă cu memorarea straturilor definite de modelul de rețea OSI, utilizați o metodă testată în timp pentru memorarea unei secvențe de cuvinte care nu au legătură între ele. Următoarele fraze „fără sens” sunt mult mai ușor de reținut decât numele straturilor, iar dacă vă puteți aminti una dintre aceste fraze, sunt șanse mari să vă aduceți aminte de straturi, în ordinea corectă, atunci când susțineți testul:

All People Seem To Need Data Processing.

Please Do Not Touch Steve's Pet Alligator.

Please Do Not Throw Sausage Pizza Away.

După cum puteți vedea, prima frază poate fi utilizată pentru a memora modelul de sus în jos (stratul aplicație, stratul prezentare, stratul sesiune și așa mai departe), în timp ce următoarele două pot fi folosite pentru a memora straturile de jos în sus (stratul fizic, stratul legătură de date, stratul rețea și așa mai departe). Mult succes la test!

Stratul legătură de date

Funcțiile executate pe acest strat sunt destinate asigurării de transmisii sigure de date de la un dispozitiv la altul în cadrul rețelei, cum ar fi verificarea de bază a apariției erorilor în cadrele transmise la nivelul fizic.

La acest nivel, biții individuali ai unui mesaj ajung la stratul fizic, iar acest strat îi organizează în formatul de cadre corespunzător, care poate fi înțeles de protocoalele de pe nivelurile superioare. Specificațiile IEEE împart acest strat în două substraturi: stratul de control al accesului la mediu (Media Access Control – MAC) și stratul de control al legăturii logice (Logical Link

Control – LLC). Deși nu fac parte din modelul OSI original, aceste substraturi joacă un rol important în cele mai multe implementări de rețele Ethernet. Substratul superior (LLC) implementează punctele de acces la servicii (Service Access Points – SAP), care pot fi referite de alte dispozitive la trimiterea de informații, iar substratul MAC este dedicat trimiterii și recepționării de date fără erori între nodurile din rețea.

Stratul rețea

Conexiunile dintre nodurile rețelei sunt controlate de acest strat. La acest nivel este stabilită și terminată o conexiune logică de rețea între noduri. Între funcțiile care formează serviciile stratului rețea se numără:

- Translatarea adreselor logice și fizice
- Rutarea și comutarea
- Controlul fluxului și evitarea congestiei rețelei
- Fragmentarea și reasamblarea pachetelor (efectuată până când se determină faptul că un ruter sau un alt dispozitiv prin care trec datele nu poate manevra pachetul la dimensiunea sa curentă)

Acest strat este cel mai de jos din modelul de referință care nu are cunoștință despre aspectele fizice de bază ale rețelei.

Stratul transport

Acest model de strat este cel mai de jos din modelul de referință care oferă servicii utilizator straturilor superioare. Pe acest strat sunt efectuate și funcțiile de calitate a serviciilor, cum ar fi:

- Transportul datelor fără erori. Datele aflate în pachete mari sunt divizate pentru a face transmisia mai eficientă. Ele sunt reasamblate pe acest strat după ce ajung aici de la un sistem situat la distanță. Conținutul pachetului depinde de protocolul utilizat de cele două noduri pentru schimbul de date.
- Secvențierea în vederea garantării livrării pachetelor în ordinea corectă către straturile superioare.
- Confirmarea transferului sau recepționării pachetelor de date.
- Controlul fluxului pentru protocolul utilizat.

Stratul sesiune

Pe acest nivel al modelului sunt stabilite și gestionate sesiuni între calculatoare. Aplicațiile trebuie să își recunoască partenerii de dialog de pe un sistem situat la distanță și să stabilească o *sesiune* comună pentru tratarea schimburilor de date. De exemplu, pe acest strat protocolul NetBIOS operează pentru a stabili sesiuni bazate pe nume. Pentru a controla o sesiune, software-ul de pe acest strat realizează un arbitraj între cele două calculatoare, comunicând fiecăruia când poate să transmită și pentru cât timp. Sesiunile dintre software-ul de aplicație sunt create, întreținute și terminate pe acest nivel.

Stratul prezentare

Modul în care sunt interpretate și prezentate datele pentru aplicație este determinat pe stratul prezentare al modelului. Informațiile trebuie să fie arătate utilizatorilor astfel încât să poată fi înțelese. Diferențele dintre noduri, cum ar fi modul de reprezentare a datelor (de exemplu, EBCDIC în comparație cu ASCII) sunt tratate aici. Pe acest strat sunt executate comprimarea datelor și conversiile de protocol. De asemenea, și criptarea este efectuată tot pe acest strat. Acest strat include și redirectorul, care „direcționează” operațiile de intrare/ieșire pentru resursele de rețea în cazul în care acestea nu se găsesc pe calculatorul local.

Stratul aplicație

Aici sunt tratate comunicațiile dintre aplicațiile utilizatorilor. Funcțiile de pe acest strat suportă aplicațiile utilizator care folosesc rețeaua. Serviciile care permit unui program să obțină acces la o bază de date care se găsește pe un server realizează aceasta apelând la funcțiile de pe acest nivel. Alte servicii de aplicații implementate la acest nivel sunt:

- Serviciile de director
- Serviciile de poștă electronică
- Serviciile de fișiere și imprimante
- Sesiunile terminale (de exemplu, Telnet)
- Serviciul de reclame
- Interprocess Communications

Cum se potrivește TCP/IP în modelul OSI?

Cu toate că modelul OSI este utilizat pe scară largă atunci când se discută de probleme referitoare la protocoale și servicii de rețea, poate fi dificil de aplicat strict la protocoalele și

serviciile care formează suita TCP/IP. Există un motiv întemeiat pentru această dificultate: dezvoltarea suitei TCP/IP a început înainte de proiectarea modelului OSI. Cu toate acestea, TCP/IP a fost proiectat pe baza unui model similar, care este numit uneori modelul DARPA sau DOD (Department of Defense).

În figura 2.2 puteți vedea cele patru straturi care formează modelul TCP/IP-DOD și modul în care pot fi relaționate cu modelul OSI.

FIGURA 2.2

Comparație între modelele de rețea TCP/IP și OSI.

Modelul OSI	Modelul TCP/IP
Aplicație	Aplicație
Prezentare	
Sesiune	
Transport	Transport
Rețea	Rețea
Legătură de date	Acces la rețea
Stratul fizic	

¹ DOD este echivalentul Ministerului Apărării în Statele Unite ale Americii (n.trad.)

Astfel, deși TCP/IP nu se potrivește exact cu modelul OSI, este posibil să faceți referire la acest model atunci când discutați anumite aspecte ale protocoalelor și serviciilor puse la dispoziție de TCP/IP.

Protocoalele TCP/IP

Așa cum s-a discutat la începutul acestui capitol, TCP/IP face referire la o suită de protocoale și aplicații, dintre care cele mai importante sunt protocolul de control al transmisiei (Transmission Control Protocol) și protocolul Internet (Internet Protocol). Vom analiza inițial protocolul Internet, deoarece este utilizat de protocoalele TCP și UDP și reprezintă baza pentru mutarea reală a datelor prin rețea.

Protocolul IP (Internet Protocol)

Protocolul Internet este a doua componentă a acronimului TCP/IP, însă este primul protocol despre care discutăm. Aceasta se datorează faptului că IP este protocolul de bază din suită utilizat pentru mutarea pachetelor dintr-un loc în altul. IP pune la dispoziție un serviciu de rețea fără conexiune și fără confirmare. Iată câteva caracteristici ale protocolului IP:

- Deoarece IP este fără conexiune, fiecare pachet este independent. IP analizează informațiile de antet ale unui pachet și folosește aceste informații pentru a trimite pachetul către destinația finală. IP nu este interesat dacă pachetele ajung în ordinea în care au fost expediate.
- IP este fără confirmare. IP nu oferă nici un mecanism pentru a determina dacă un pachet mai ajunge la destinație. Protocolul nu face decât să trimită pachetul și presupune fie că aceasta va ajunge unde trebuie, fie că un alt protocol va fi responsabil pentru această verificare.
- IP nu este interesat de calea pe care circulă un pachet atunci când traversează Internetul. Deciziile de rutare sunt lăsate de obicei în seama altor protocoale. Este foarte posibil ca pachete provenite de la același calculator gazdă să parcurgă rute diferite către aceeași destinație.

Deci, vă puteți întreba cu ce se ocupă de fapt protocolul IP. IP preia datele de pe stratul gazdă-la-gazdă și le fragmentează în pachete (denumite *datagrame*) de o dimensiune care poate fi transferată prin rețea. La destinație, IP reassemblează aceste datagrame și le transferă în sus în stiva de protocoale. Pentru ca fiecare pachet să fie livrat, protocolul Internet plasează adresele IP sursă și destinație în antetul pachetului. De asemenea, efectuează un calcul al sumei de control a informațiilor din antet pentru a se asigura de corectitudinea acestora, însă nu efectuează această funcție și pentru zona de date a pachetului.

Când discutați despre o adresă de rețea din Internet, discutați de o adresă IP. Ulterior în acest capitol, voi explica funcționarea adresării IP și de ce este atât de potrivită pentru Internet care este format din numeroase rețele diferite.

Ce înseamnă încapsulare?

TCP/IP oferă posibilitatea de interoperare pentru rețelele de calculatoare realizate cu tehnologii de bază diferite. De exemplu, s-ar putea ca o rețea să utilizeze formatul de cadru Ethernet 802, în timp ce alta utilizează FDDI. Fiecare dintre aceste cadre de nivel scăzut are propriul antet, specific, care conține informațiile necesare tehnologiei

respectiv pentru a trimite cadre prin rețeaua fizică. La acest nivel scăzut din stiva de protocoale, datagrama IP intră în zona de date a cadrului. Cu alte cuvinte, după ce protocolul IP adaugă informațiile de antet și creează o datagramă de dimensiune corespunzătoare, transferă datagrama către stratul acces la rețea, care introduce datagrama IP într-un cadru Ethernet, de exemplu. La destinație, informațiile de antet din cadrul Ethernet sunt eliminate, iar datagrama IP este transferată pe nivelul superior din stivă pentru a fi prelucrată de protocolul IP.

Atunci când configurați un ruter cu funcția de filtrare a pachetelor, informațiile de antet IP sunt cele utilizate pentru a lua decizii în ceea ce privește transferul sau respingerea pachetului.

Protocolul de control al transmisiei (TCP)

Acest protocol utilizează protocolul IP și pune la dispoziție un serviciu fiabil de conexiune între două calculatoare gazdă din Internet. În timp ce protocolul IP trimite pur și simplu pachetele pe rutele lor, TCP oferă mecanismele care garantează că pachetele sunt recepționate intacte și că pot fi plasate în ordinea corectă la calculatorul destinație.

Protocolul TCP pune la dispoziție sume de control pentru datele reale transmise. De asemenea, TCP posedă mecanisme care regularizează fluxul de date pentru a evita problemele asociate cu congestia. TCP folosește numere secvențiale în antetul TCP pentru ca datagramele IP să poată fi reasamblate în ordinea corectă la capătul destinației al comunicației.

Alte protocoale care au legătură cu TCP/IP

TCP și IP nu sunt singurele protocoale din această suită. În timp ce combinația TCP/IP oferă un canal de comunicație de la un calculator la altul în Internet, există și alte protocoale utilizate pentru a executa sarcini specifice.

Protocolul UDP (User Datagram Protocol)

User Datagram Protocol (UDP) este similar cu TCP prin faptul că folosește protocolul IP pentru a muta pachetele prin rețea. UDP nu pune la dispoziție un mecanism de confirmare, așa cum procedează TCP, astfel că poate fi considerat un serviciu *fără conexiune*. Pentru aplicațiile care nu au nevoie de un serviciu de livrare garantat (și de informațiile suplimentare asociate acestuia) poate fi utilizat protocolul UDP. Un exemplu în acest sens este serviciul de nume de domenii (Domain Name Service, sau DNS). DNS utilizează pachete UDP pentru a putea schimba eficient informații cu alte calculatoare.

Protocolul ARP (Address Resolution Protocol)

Natura funcției de adresare IP ușurează rutarea datelor prin Internet. Atunci când un pachet este trimis către o rețea diferită de cea în care a fost generat, este transferat unui ruter. Ruterul ia decizii pe baza adresei IP și a informațiilor pe care le posedă în tabelul de rutare pentru a trimite pachetul pe drumul către segmentul de rețea corect. Uneori, ruterul nu are o conexiune directă cu rețeaua destinație, astfel că expediază pachetul către un alt ruter care poate să execute această funcție. Când pachetul se îndreaptă în sfârșit către segmentul de rețea corect, ruterul sau poarta locală trebuie să cunoască adresa hardware (adresa MAC) a calculatorului destinație, astfel încât pachetul să facă ultimul pas din călătorie.

Adresele IP sunt utilizate pentru a forma un spațiu ierarhic de adrese care poate fi înțeles de agenții de rutare din Internet, astfel încât aceștia să poată determina modul în care să transmită un pachet dintr-o rețea în alta. Când dispozitivele comunică direct pe segmentul de rețea local (pe sârmă, să spunem așa), adresa reală utilizată pentru comunicarea între două dispozitive, indiferent dacă acestea sunt calculatoare, rutere sau orice altceva, este adresa internă de control al accesului la mediu (Media Access Control, sau MAC).

Protocolul de rezolvare a adreselor (Address Resolution Protocol, sau ARP) este folosit pentru a realiza traducerea (corespondența) între adresele IP și adresele hardware. Când un calculator vrea să trimită un pachet către un alt dispozitiv, trebuie să știe adresa MAC a acestuia. Pentru a afla această adresă MAC, trimite un mesaj de difuzare pe care îl poate vedea orice calculator din segmentul local. Acest mesaj ARP conține adresa MAC a calculatorului de origine, precum și adresa IP a calculatorului cu care vrea să comunice acesta. Când un calculator recunoaște propria adresă IP în acest pachet de difuzare, trimite către calculatorul care a emis pachetul ARP un pachet în care include propria adresă MAC. Din acest moment, fiecare dintre cele două calculatoare cunoaște adresa MAC a celuilalt și comunicațiile ulterioare se fac folosind aceste adrese.

Pentru a preveni o rafală de mesaje de difuzare care ar putea rezulta dacă aceste operații au loc pentru fiecare pachet care trebuie livrat în segmentul local de rețea, fiecare gazdă păstrează un timp în memorie un tabel de adrese MAC. Atunci când trebuie să comunice cu un alt calculator, acest tabel ARP este primul loc verificat. Dacă adresa destinație nu este găsită în tabelul ARP, este utilizată metoda de difuzare ARP.

Comanda arp, care se găsește atât în sistemul de operare UNIX, cât și în Windows NT, vă permite să vizualizați tabelul ARP. De asemenea, poate fi folosită pentru a adăuga sau a șterge intrări din tabel. Cu toate că sintaxa variază între sisteme de operare diferite, în majoritatea sistemelor sunt valabile următoarele forme:

- arp -a Afișează conținutul curent al tabelului ARP.
- arp -d *adresa_IP* Șterge intrarea pentru gazda specificată.
- arp -s *adresa_IP adresa_ether* Adaugă intrarea în tabel.

De exemplu, pentru a adăuga o intrare, folosiți următoarea sintaxă:

```
arp -s 192.113.121.88 08-00-2b-34-c1-01
```

Numele de gazdă, cum este www.microsoft.com, și adresele IP sunt utilizate pentru a simplifica configurarea și gestionarea unei rețele într-un mod ordonat. Pe cel mai mic nivel este adresa MAC hardware folosită de plăcile de rețea pentru a discuta una cu cealaltă. Imaginați-vă ce ar fi Internetul dacă fiecare ar trebui să memoreze adresele hardware (în locul numerelor). Deoarece adresa MAC este pur și simplu o serie de numere „imprimate” în adaptorul de rețea în momentul fabricării, nu are nici o legătură cu locația reală a calculatorului sau a altui dispozitiv de rețea. Ca urmare, pentru a ruta mesaje prin Internet folosind doar aceste adrese MAC codate în hardware ar fi necesar ca un ruter să memoreze un tabel enorm care ar conține adresele MAC ale tuturor calculatoarelor care există în Internet. Desigur, o sarcină imposibilă!

Protocolul ICMP (Internet Control Message Protocol)

Cu toate că protocolul IP nu oferă mecanisme de confirmare pentru a permite calculatorului care a trimis mesajul să afle dacă datagrama a fost recepționată intactă la destinație, pune la dispoziție o serie de mecanisme de raportare a erorilor, prin intermediul protocolului ICMP (Internet Control Message Protocol). Este o componentă necesară a

oricărei implementări TCP/IP, iar funcțiile pe care le efectuează sunt foarte importante pentru rutere și alte dispozitive de rețea care comunică prin TCP/IP. Ca și TCP și UDP, ICMP folosește protocolul IP pentru a transmite propriile date prin rețea.

Dacă ați utilizat vreodată comenzile PING și TRACEROUTE, înseamnă că ați folosit protocolul ICMP.

Fiecare pachet ICMP are un câmp care definește tipul mesajului. Tipurile de mesaje folosite de acest protocol sunt prezentate în tabelul 2.1. În plus, fiecare pachet ICMP conține și un câmp de cod, întrebuițat pentru detalii suplimentare referitoare la tipul de mesaj.

Tabelul 2.1 Tipuri de mesaje ICMP

Tip de mesaj	Descriere
0	Echo Reply (Răspuns de ecou)
3	Destination Unreachable (Destinație inaccesibilă)
4	Source Quench (Oprirea sursei)
5	Redirect Message (Redirecționarea mesajului)
8	Echo Request (Cerere de ecou)
11	Time Exceeded (Depășirea timpului)
12	Parameter Problem (Problemă legată de parametru)
13	Timestamp Request (Cerere de marcă de timp)
14	Timestamp Reply (Răspuns de marcă de timp)
15	Information Request (Cerere de informații) – nu mai este folosit în prezent
16	Information Reply (Răspuns de informații) – nu mai este folosit în prezent
17	Address Mask Request (Cerere de mască de adresă)
18	Address Mask Reply (Răspuns de mască de adresă)

Comanda PING folosește mesajele de cerere și răspuns la ecou pentru a stabili dacă există o conexiune fizică între sisteme. O altă funcție importantă în Internet este controlul traficului. Mesajul de oprire a sursei poate fi transmis pentru a comunica unei gazde sursă că gazda destinație nu poate ține pasul cu viteza de transmitere a pachetelor. Calculatorul destinație continuă să transmită aceste mesaje de oprire până când sursa reduce viteza de transmisie la o valoare acceptabilă.

Ruterele folosesc o altă funcție ICMP valoroasă pentru a comunica unui alt ruter că știu o cale mai bună până la destinație. Aceasta se realizează folosind mesajele de redirecționare. Ruterele pot folosi, de asemenea, mesajele de depășire a timpului pentru a indica unui alt dispozitiv de ce un pachet a fost respins.

În afară de rutere și alte dispozitive intermediare, și gazdele pot folosi protocolul ICMP. De exemplu, atunci când un calculator este încărcat și nu știe care este masca de rețea pentru rețeaua locală, poate genera un mesaj de cerere a măștii de adrese. Un alt dispozitiv din rețea poate răspunde acestui mesaj pentru a ajuta calculatorul aflat în dificultate.

În tabelul 2.1, mesajele pentru cereri de informații și răspuns la acestea sunt incluse numai pentru o prezentare completă. Rolul acestora era inițial de a permite unei gazde să obțină o adresă IP, dar această funcție este acum asigurată de protocoalele bootp și DHCP (Dynamic Host Configuration Protocol).

Adresarea IP

Adresele IP sunt utilizate pentru a oferi un spațiu ierarhic de adrese pentru Internet. Fiecare adaptor de rețea are o adresă de rețea codată în hardware, cu lungimea de șase octeți. Această adresă este imprimată în cursul procesului de fabricație. Când pachetele de date sunt trimise pe cablu în segmentul local de rețea, adresa MAC (Media Access Control) este cea folosită efectiv pentru adresele sursă și destinație înglobate în cadrul Ethernet, care încapsulează datagrama IP propriu-zisă.

Singura componentă semnificativă a adresei MAC este formată din primii trei octeți, care identifică producătorul plăcii. Ceilalți trei octeți sunt folosiți pur și simplu pentru a identifica în mod unic fiecare dispozitiv.

Termenii adresă MAC, adresă fizică și adresă hardware sunt interschimbabili. Fiecare dintre acești termeni face referire la adresa „imprimată” de producător în fiecare placă fabricată.

Adresa MAC alocată fiecărei plăci de rețea este unică. Aceasta este o adresă pe 6 octeți, exprimată de obicei în cifre hexazecimale, pentru a fi mai ușor de scris. De exemplu, este mult mai ușor să scrieți 00-80-C8-EA-AA-7E decât să exprimați aceeași adresă în binar (ceea ce vede rețeaua) sub forma unui șir de 0 și 1, cu lungimea de 48 de caractere.

Clasele de adrese IP

Internet este o colecție de rețele individuale conectate împreună. Protocolul Internet, după cum sugerează și numele, este folosit pentru schimburile de date între rețele. Amintiți-vă că toate comunicațiile din segmentul local de rețea au loc folosind adresele MAC. Dacă nu ar fi necesară conectarea rețelelor mici într-o structură mai mare, adresarea ar putea fi destul de simplă. Pentru identificarea unică a fiecărui calculator din rețea ar putea fi folosite fie adresele MAC, fie o schemă simplă de numerotare (1, 2, 3...). Oricum, protocolul IP permite calculatoarelor din diferite tipuri de rețele să schimbe date între ele.

O adresă IP are lungimea de 4 octeți (32 de biți). În timp ce adresele MAC sunt exprimate de obicei în notația hexazecimală, adresele IP sunt exprimate de obicei într-un format numit notație zecimală cu puncte. Aceasta înseamnă că fiecare octet din adresă poate fi transformat în reprezentarea sa zecimală, iar cei patru octeți ai adresei sunt separați prin puncte pentru a fi mai ușor de reținut. Tabelul 2.2 arată care este legătura dintre valorile zecimale și valorile binare ale adresei de 32 de biți 10001100101100001101100110010100.

Tabelul 2.2 Adrese IP exprimate în notație zecimală

Valoare zecimală	Valoare binară
140	10001100
176	10110000
217	11011001
148	10010100

Așa cum puteți vedea, este mult mai ușor să scrieți adresa în notație zecimală cu puncte (140.176.217.148) decât să folosiți echivalentul binar.

Deoarece adresa IP este utilizată pentru a ruta un pachet printr-o colecție de rețele separate, o parte a adresei IP este folosită pentru a identifica rețeaua, iar cealaltă parte a adresei pentru identificarea calculatorului. Pentru a complica puțin lucrurile, adresele IP sunt împărțite în trei clase importante (A, B și C) și alte două mai puțin cunoscute (D și E). Fiecare clasă folosește un număr diferit de biți din adresa IP pentru identificarea rețelei.

Pentru a identifica diferitele clase de rețea sunt folosiți primii câțiva biți ai adresei.

Deoarece numărul total de biți disponibili pentru adresare este întotdeauna același (32), utilizarea unui număr diferit de biți pentru identificarea rețelei implică faptul că unele clase pot să identifice mai multe rețele decât altele. De asemenea, unele clase pot să identifice mai multe calculatoare în fiecare rețea.

Puteți spune cărei clase îi aparține o adresă examinând primii patru biți ai adresei. Tabelul 2.3 prezintă clasele de adrese IP, în funcție de valorile primilor patru biți. În acest tabel, pozițiile biților marcate cu „x” indică faptul că valoarea respectivă nu contează în determinarea clasei de adrese IP.

Tabelul 2.3 Clasele de adrese IP, determinate de primii patru biți

Clasa IP	Valoarea primului octet
Clasa A	0xxx
Clasa B	10xx
Clasa C	110x
Clasa D	111x
Clasa E	1111

Orice adresă IP care are valoarea 0 pe poziția primului bit este o adresă din clasa A, indiferent de valorile celorlalți trei biți din adresă. Orice adresă care începe cu valoarea 10 este o adresă din clasa B și așa mai departe. Amintiți-vă că acestea sunt valori de biți și sunt exprimate în binar. Ele nu sunt valorile zecimale ale adresei IP folosite în notația zecimală cu puncte.

Adrese de clasă A

Intervalul pentru adresele din clasa A începe de la o combinație cu toți cei 32 de biți având valoarea 0, până la o combinație cu 0 pe prima poziție și restul biților având valoarea 1. Dacă luați fiecare octet și îl transformați în zecimal, veți vedea că adresele din clasa A, exprimate în notația zecimală cu punct, pot varia de la 0.0.0.0 la 127.255.255.255.

Primul octet din adresele de clasă A este folosit pentru reprezentarea porțiunii de rețea a adresei, iar ceilalți trei octeți sunt folosiți pentru identificarea fiecărui calculator din rețea. Deoarece primul bit al primului octet al adresei are întotdeauna valoarea 0, mai rămân numai 7 biți cu care poate fi creată o adresă de rețea. Ca urmare, într-o rețea de clasă A pot exista numai 127 de adrese de rețea (01111111 în binar). Nu pot exista 128 de adrese de rețea în această clasă, deoarece numărul 128 exprimat în binar este 10000000, care indică o adresă din clasa B.

Deoarece primul octet din adresa de clasă A este folosit pentru identificarea adreselor de rețea, rămân trei octeți care pot fi folosiți pentru identificarea calculatoarelor din rețea. Cea mai mare valoare pe care o puteți exprima folosind 3 octeți este un șir de 24 de 1. În zecimal, această valoare este 16.777.215. Dacă numărați și valoarea zero (intervalul devenind astfel 0-16.777.215), aceasta înseamnă un total de 16.777.216 (2 la puterea 24) adrese ce pot fi exprimate folosind cei 3 octeți.

Acest număr înseamnă o mulțime de adrese de calculator! Ca urmare, pot exista în total 127 de rețele de clasă A (identificate după primul octet al adresei de clasă A), fiecare rețea putând avea până la 16.777.216 adrese unice pentru calculatoarele din rețea. Astfel, domeniul de valori pentru rețelele de clasă A variază de la 0.0.0.0 la 127.255.255.255. Dacă vedeți o adresă din acest domeniu, puteți fi sigur că este o adresă de clasă A.

Valoarea unui octet cu toți biții 1 (11111111) este 255 în notație zecimală. De aici puteți deduce că nici o adresă IP nu poate avea vreun octet mai mare decât această valoare. De exemplu, adresa 140.176.123.256 nu este o adresă IP validă, deoarece ultimul octet este mai mare decât valoarea zecimală 255. Rețineți acest lucru atunci când vă gândiți cum să distribuiți adresele IP pentru rețeaua dumneavoastră!

Adrese de clasă B

Această clasă de adrese poate fi identificată atunci când primii doi biți ai adresei au valoarea „10”. O adresă din clasa B, exprimată în binar, poate varia de la o combinație de biți care începe cu 1 și este urmată de 31 de 0, până la 10, urmat de 30 de 1. Exprimat în notația zecimală cu punct, acest interval variază de la 128.0.0.0 până la 191.255.255.255. Valoarea 128 în zecimal este 10000000 în binar. Valoarea 191 în zecimal este 10111111 în binar.

În adresele din clasa B, primii doi octeți ai adresei sunt utilizați pentru identificarea rețelei, iar ultimii doi octeți sunt lăsați pentru crearea adreselor calculatoarelor din rețea. Folosind cei doi octeți, în această clasă pot exista 16.384 de adrese de rețea (de la 128.0 la 191.255) și 65.536 (2 la puterea 16) de calculatoare individuale în fiecare rețea din clasa B.

Ținând cont de faptul că porțiunea pentru rețea și porțiunea pentru calculatoare gazdă din adresa de clasă B au ambele lungimea de 2 octeți, de ce apare o diferență între numărul de rețele adresate și numărul de calculatoare gazdă care pot fi adresate? Aceasta se datorează faptului că adresa de clasă B are întotdeauna valoarea 1 pentru primul bit și valoarea 0

pentru al doilea bit. În plus, și alte clase de adrese sunt definite utilizând primii trei sau patru biți ai adresei. Această regulă elimină o parte din valorile posibile pe care le puteți crea cu ajutorul a doi octeți pentru obținerea unei adrese de rețea.

Pe scurt, adresele din clasa B pot avea valori între 128.0.0.0 și 191.255.255.255.

Adrese de clasă C

Adresele din clasa C încep întotdeauna cu valoarea 110 pentru primii trei biți. Dacă transformați această valoare în zecimal, puteți vedea că adresele de rețea din clasa C pot avea valori între 192.0.0.0 și 223.255.255.255. Primii trei octeți ai unei adrese din clasa C reprezintă partea de rețea a adresei și numai ultimul octet rămâne disponibil pentru crearea adreselor de gazde.

Făcând un calcul simplu, puteți vedea că pot exista până la 2.097.152 de rețele din clasa C, fiecare având cel mult 256 de calculatoare gazdă (în intervalul 0-255). Această împărțire asigură un număr mare de rețele de clasă C, fiecare având un număr mic de calculatoare.

Clasele D și E

Clasele D și E sunt folosite diferit față de clasele A, B și C. Adresele din clasa D sunt rezervate pentru difuzările pe grupuri (multicast). Procesul de transmitere a unui pachet de rețea către mai multe calculatoare gazdă se numește *multicasting*. Adresele din clasa D pot avea valori, în zecimal, între 224.0.0.0 și 239.255.255.255.

Într-o adresă din clasa D nu există octeți alocați anume porțiunii de rețea sau de gazdă a adresei. Aceasta înseamnă că pot fi create 268.435.456 de adrese unice de clasă D.

Adresele din clasa E pot fi identificate după valorile 1 stabilite pentru biții de pe primele patru poziții. În zecimal, această clasă are valori între 240.0.0.0 și 255.255.255.255, valoarea maximă pe care o puteți exprima în binar folosind numai 32 de biți. Adresele din clasa E sunt rezervate pentru utilizări viitoare și, în mod normal, nu sunt folosite în rețelele conectate prin Internet.

Adrese pentru rețelele private

A devenit clar la începutul anilor '90 că spațiul de adrese IPv4 s-ar putea epuiza mult mai repede decât s-a preconizat. În documentul RFC¹ 1918, „Alocarea adreselor pentru rețelele Internet private”², se discută despre utilizarea câtorva domenii de adrese IP pentru rețelele private care nu trebuie să comunice direct pe Internet. Aceste domenii sunt următoarele:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

¹ RFC = Acronim pentru Request for Comments (Invitație la discuții). Document în care este publicat un standard, un protocol sau alte informații referitoare la funcționarea Internetului. În realitate, este emis sub controlul organismului Internet Architecture Board după discuții și are rolul de standard. (n.trad.)

² În original, „Address Allocation for Private Internets” (n.trad.)

Deoarece în prezent aceste adrese nu mai sunt valide în Internet, ele pot fi utilizate de mai multe rețele private. Pentru a conecta rețeaua privată la Internet, puteți folosi unul sau mai multe servere intermediare.

Vezi și

➤ *Vezi capitolul 7, „Porți de aplicații și servere intermediar”, la pagina 132, pentru mai multe informații despre modul în care se realizează această alocare.*

Adrese de difuzare și de difuzare pe grupuri

Până în acest moment, am identificat domeniile de adrese care pot fi utilizate pentru a crea adresele IP din diferite clase. Însă există și excepții care trebuie remarcate. O adresă care identifică în mod unic un calculator din Internet se numește adresă *unică* (*unicast*).

Numărul total de adrese unice din fiecare clasă va fi mai mic decât credeți, deoarece unele adrese sunt rezervate de obicei pentru scopuri speciale. De exemplu, orice adresă în care primul octet are valoarea 127 nu este o adresă validă în afara calculatorului gazdă local. Adresa 127.0.0.1 (care din punct de vedere tehnic este o adresă de clasă A) este numită de obicei *adresă de buclă* (*loopback address*) și poate fi folosită pentru testarea stivei TCP/IP de pe calculator. Când trimiteți un pachet către această adresă (folosind comanda PING, de exemplu), acesta nu iese din adaptorul local de rețea pentru a fi distribuit în rețea. Pachetul nu face decât să traverseze stiva de protocoale înainte și înapoi pentru a testa configurarea corespunzătoare a calculatorului local.

Această adresă poate fi folosită și cu alte utilitare TCP/IP decât PING. De exemplu, folosind această adresă puteți transmite un mesaj telnet către calculatorul local pentru a testa funcționalitatea serverului telnet local.

În general, nu folosiți valorile 0 sau 255 pentru nici unul din cei patru octeți ai unei adrese IP. Dacă este folosită în porțiunea de rețea a unei adrese, valoarea zero implică rețeaua curentă.

Valoarea 255 este folosită în adrese pentru a specifica un mesaj difuzat. Acest tip de mesaj este transmis o singură dată, dar poate fi recepționat de mai multe gazde. Difuzările pot fi folosite pentru transmiterea unui pachet către toate calculatoarele dintr-o anumită rețea sau subrețea. De exemplu, un pachet cu adresa 10.11.255.255 va fi recepționat de toate calculatoarele gazdă din rețeaua definită de 10.11.

Tabelul 2.4 prezintă numărul de adrese rămase de fapt pentru clasele A-C după extragerea adreselor speciale.

Tabelul 2.4 Adrese IP disponibile

Clasă	Număr de rețele	Număr de gazde
A	126	16.777.214
B	16.384	65.534
C	2.097.152	254

Ce sunt subrețelele?

Spațiul de adrese IP este foarte valoros. Pentru ca o firmă (sau un furnizor de servicii Internet) să creeze mai multe rețele, s-ar părea că este nevoie de mai multe domenii de adrese. Însă există o metodă de adresare, denumită lucrul cu subrețele (subnetting), care poate fi utilizată pentru a lua un singur spațiu contiguu de adrese și a-l împărți în mai multe rețele denumite *subrețele* (subnets). De exemplu, o adresă de clasă B poate avea până la 65.534 de calculatoare gazdă pe un segment de rețea. Puțină lume are nevoie de atâtea calculatoare într-o singură rețea. Folosirea unui astfel de domeniu pentru o rețea mică ar putea fi o risipă enormă.

Deși clasele de adrese IP au fost stabilite astfel încât să simplifice identificarea fiecărei porțiuni a adresei IP care a fost folosită pentru identificarea adresei de rețea și a calculatorului gazdă, există nevoia de stabilire a părții de adresă care este folosită pentru identificarea subrețelei. Aceasta se realizează cu ajutorul unei *măști de subrețea* (subnet mask). O mască de subrețea este o valoare binară pe 32 de biți utilizată special în acest scop.

Măști de subrețea de clasă A, B și C

O mască de subrețea poate fi utilizată pentru a „împrumuta” câțiva biți din porțiunea de gazdă a adresei IP astfel încât să poată fi folosiți pentru identificarea rețelei sau subrețelei. Masca de subrețea este o valoare exprimată în format zecimal cu punct, la fel ca o adresă IP, iar rolul acesteia este de a „masca” porțiunea din adresa IP care specifică rețeaua și partea de subrețea a adresei.

De exemplu, clasele de adrese A, B și C, care au fost descrise mai devreme, au asociate măști specifice. Masca adreselor din clasa A este 255.0.0.0. Deoarece 255 este reprezentat în binar ca un șir de opt biți cu valoarea unu, reprezentarea binară a acestei măști este 11111111000000000000000000000000. Folosind logica booleană, această mască de subrețea în format binar poate fi utilizată împreună cu operatorul AND pentru a masca porțiunile de rețea și subrețea dintr-o adresă IP. Folosind operatorul AND, se va obține rezultatul TRUE numai dacă ambele argumente au valoarea TRUE.

Dacă valoarea TRUE este reprezentată de numărul 1 și valoarea FALSE este reprezentată de numărul 0, este ușor pentru un calculator sau un ruter să aplice masca adresei IP pentru a obține porțiunea de rețea a adresei. Tabelul 2.5 arată cum sunt obținute valorile finale.

Tabelul 2.5 Logica booleană folosită pentru măștile de subrețea

Valoarea adresei IP	Valoarea măștii	Rezultat
1	1	1
1	0	0
0	1	0
0	0	0

Puteți observa că atunci când aplicați masca de subrețea 255.0.0.0 unei adrese din clasa A, singura porțiune din adresa IP care este selectată pentru adresa rețelei este cea conținută în primul octet.

Vă puteți da seama ușor că masca de subrețea pentru adresele din clasa B este 255.255.0.0, iar pentru adresele din clasa C este 255.255.255.0. Fiecare dintre aceste măști de subrețea blochează doar porțiunea din adresa IP stabilită deja pentru clasa respectivă că este folosită ca adresă de rețea. Prin modificarea valorii măștii de subrețea, puteți masca biții suplimentari care formează partea dedicată gazdei în adresă și astfel puteți împărți un spațiu mare de adrese în componente mai mici.

Subdivizarea unei adrese folosind măștile de subrețea

Împărțirea în subrețele devine utilă atunci când luați un anumit spațiu de adrese de rețea și îl împărțiți în subrețele separate.

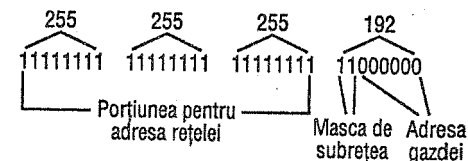
De exemplu, masca de subrețea 255.255.255.128 poate fi folosită pentru împărțirea unui spațiu de adrese din clasa C în două subrețele distincte. Dacă această mască este aplicată adresei de rețea 192.113.255, obțineți o subrețea cu adrese de gazde între 192.113.255.1 și 192.113.255.128 și o altă subrețea cu adrese de gazde între 192.113.255.129 și 192.113.255.254. (În acest exemplu au fost eliminate adresele care au în ultimul octet numai valori 0 sau numai valori 1, deoarece aceste adrese sunt cazuri speciale și, în general, nu pot fi folosite ca adrese de gazde; de exemplu, 192.113.255.0).

Într-un alt exemplu, puteți vedea că o mască de subrețea cu valoarea 255.255.255.192 va împărți un spațiu de adrese de rețea din clasa C în patru subrețele, fiecare având la dispoziție 62 de adrese de gazde. Pentru a înțelege acest lucru, priviți reprezentarea binară a numărului 192, care este 11000000. Deoarece primii 2 biți au valoarea 1, când este aplicată masca rămân numai 6 biți care pot fi folosiți pentru adresele de gazde. Cel mai mare număr care poate fi stocat pe șase biți este 63. Deoarece nu puteți folosi o adresă de gazdă care conține numai unu sau numai zero, pentru adresarea gazdelor rămân numerele de la 1 la 62.

În figura 2.3 puteți vedea că adresa IP este acum formată din trei părți: adresa de rețea, adresa de subrețea și adresa de gazdă.

FIGURA 2.3

O mască de subrețea poate fi folosită pentru a identifica porțiunile pentru adresa de rețea, adresa de subrețea și adresa gazdei din adresa IP.



Nu vreau să fac toate calculele astea!

Dacă nu doriți să vă pierdeți timpul calculând valorile subrețelelor, puteți studia un document RFC care vă poate ajuta. Căutați în Internet documentul RFC 1878, „Tabelul de subrețele de lungime variabilă pentru protocolul IPv4”¹. Acest document conține o listă cu valorile posibile pentru măștile de subrețea și vă arată cum pot fi utilizate. De asemenea, puteți să căutați în Internet produsele shareware denumite *calculatoare de subrețea* (subnet calculators), pe care le puteți folosi pentru efectuarea calculelor respective.

¹ În original, „Variable Length Subnet Table for IPv4” (n.trad.)

Cum se calculează adresele de subrețea

Pentru a împărți în subrețele un spațiu de adrese, trebuie să stabiliți inițial numărul de adrese de gazde de care aveți nevoie în fiecare subrețea și să exprimați acest număr în binar. Așa veți vedea de câți biți aveți nevoie pentru porțiunea de gazdă a spațiului de adrese. Scădeți valoarea obținută din numărul de biți disponibili (8, dacă împărțiți în subrețele ultimul octet al unei adrese din clasa C). Apoi calculați echivalentul în zecimal al numărului binar care conține pe primele poziții rămase numai biți cu valoarea 1.

De exemplu, pentru a crea subrețele care au fiecare câte 30 de adrese de gazde, va trebui să știți care este valoarea binară a numărului 30. Este 11110, ceea ce înseamnă 5 biți în binar. Ca urmare, rămân 3 biți care trebuie mascați pentru a crea porțiunea submăștii de rețea a adresei ($8-5=3$). Reprezentarea binară a măștii este 11100000, ceea ce înseamnă 224 în zecimal.

Câte subrețele puteți crea folosind această mască? Deoarece sunt utilizați doar 3 biți pentru identificarea subrețelei, cel mai mare număr pe care îl puteți reprezenta este 7 (111 în binar = 7 în zecimal). Dacă includeți și valoarea 0, obțineți 8 adrese de subrețea posibile.

Ca urmare, dacă folosiți masca 255.255.255.224 pentru împărțirea în subrețele a unei adrese IP din clasa C, puteți avea 8 subrețele, fiecare cu 30 de adrese de gazde. Care vor fi însă adresele efective de gazde din fiecare subrețea? Adresa primei subrețele este 000. Deoarece adresa IP este exprimată în notația zecimală cu punct, calculați câte adrese pot fi stocate într-o valoare binară pe 8 biți care începe întotdeauna cu 000, apoi transformați-le în zecimal, astfel:

de la 00000001 la 00011110, ceea ce înseamnă de la 1 la 30 în zecimal.

Adresele 00000000 și 00011111 nu sunt valide, deoarece au ca rezultat adrese de gazde care conțin numai 0, respectiv numai 1. Dacă această mască ar fi aplicată adresei de rețea din clasa C 192.113.255.0, gazdele din prima subrețea ar avea adrese de la 192.113.255.1 la 192.113.255.30.

Utilizând această mască, a doua adresă de subrețea este 001. Domeniul adreselor de gazde care pot fi create pentru această subrețea este următorul:

de la 00100001 la 00111110, ceea ce înseamnă de la 33 la 62 în zecimal.

În urma aplicării acestei măști de subrețea, gazdele din a doua subrețea pot avea adrese între 192.113.255.33 și 192.113.255.62.

A treia adresă de subrețea este 010. Domeniul adreselor de gazde este următorul:

de la 01000001 la 01011110

Aceasta înseamnă de la 65 la 94 în zecimal. Domeniul adreselor de gazde pentru a treia subrețea este cuprins între 192.113.255.65 și 192.113.255.94.

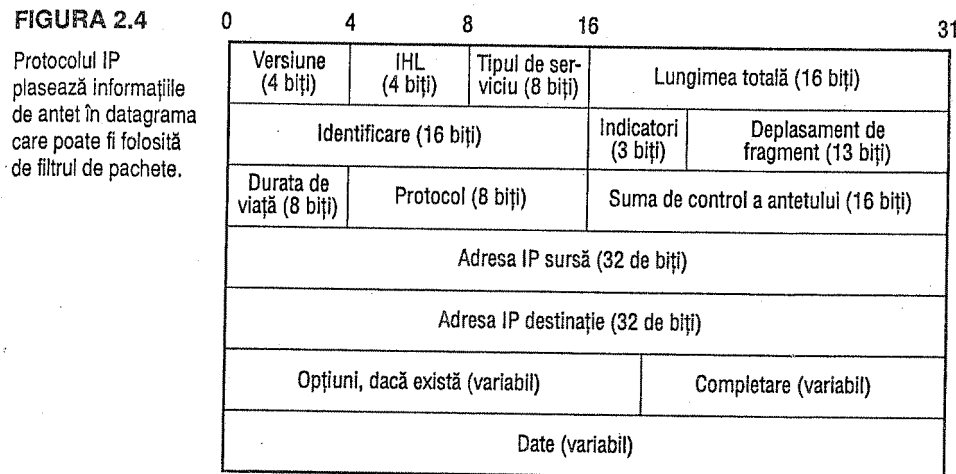
Continuând calculele pentru celelalte subrețele (de la 011 la 111), veți vedea că aveți 8 subrețele, fiecare cu 30 de adrese disponibile pentru gazde.

Puteți continua împărțirea spațiului de adrese până când ajungeți să folosiți 6 biți pentru masca de subrețea. Aceasta lasă la dispoziție numai 2 adrese pentru gazde (deoarece nu puteți folosi adresele care au numai 0 sau numai 1). Însă împărțirea în subrețele cu numai 2 gazde nu este chiar o idee practică.

Analiza conținutului unei datagrame IP

După ce un cadru este recepționat de un adaptor de rețea pe stratul fizic, informațiile de antet ale cadrului, care nu sunt relevante pentru protocolul IP, sunt eliminate, iar pachetul IP este transferat în sus în stiva de protocoale. În figura 2.4 puteți vedea structura unui pachet IP.

FIGURA 2.4



Când stratul IP recepționează datagrama, nu știe nimic despre informațiile de antet ale cadrului și folosește informațiile din antetul IP pentru o diversitate de funcții. Este important să înțelegeți conținutul antetului IP dacă doriți să înțelegeți cum funcționează un filtru de pachete, deoarece pe aceste informații se bazează deciziile filtrului. Câmpurile din antetul unui pachet IP sunt următoarele:

- **Versiune** – Acest câmp indică versiunea protocolului IP care a construit datagrama. Câmpul are lungimea de 4 biți. În prezent, cea mai utilizată versiune IP este versiunea 4. „Următoarea generație” IP este numită IPv6, prescurtare de la versiunea 6. Versiuni diferite de IP folosesc formate diferite pentru informațiile de antet. Datorită acestui aspect, dacă stratul IP de la capătul destinație este o versiune mai mică (adică mai veche) decât cea specificată în acest câmp, va refuza pachetul. Acesta este însă un eveniment rar, deoarece în prezent majoritatea sistemelor folosesc versiunea 4 a protocolului IP.
- **Lungimea antetului Internet (Internet Header Length, sau IHL)** – Acest câmp conține lungimea antetului pachetului și poate fi utilizat de programele software pentru a calcula locul în care începe efectiv zona de date în cadrul datagramei. Lungimea este exprimată ca un număr de cuvinte pe 32 de biți. Acest câmp are lungimea de 4 biți.
- **Tipul de serviciu** – Acest câmp de 8 biți a fost creat pentru ca protocolul IP să poată determina modul de tratare a unei anumite datagrame, cum ar fi acordarea unei priorități mai mici sau mai mari pentru un pachet. Însă nici o implementare importantă a protocolului IP versiunea 4 nu folosește biții din acest câmp, astfel încât în mod uzual li se atribuie valoarea 0.

- **Lungimea datagramelor** – Acest câmp este folosit pentru a specifica lungimea întregii datagramă și este exprimat într-un număr de octeți (bytes). Deoarece are lungimea de 16 biți, poate fi folosit pentru a specifica o dimensiune de pachet de până la 65.534 de octeți. Scăzând valoarea câmpului IHL din această valoare IP, poate fi determinată lungimea zonei de date a datagramelor.
- **Identificare** – Atunci când protocolul IP împarte un mesaj în mai multe datagramă astfel încât să poată fi transmise prin rețea (operație denumită fragmentare), trebuie să cunoască la capătul de destinație ce datagramă aparțin aceluiași mesaj, astfel încât să poată fi reasamblate. Pentru acest scop este utilizat acest câmp. Calculatorul expeditor va folosi un număr unic pentru fiecare mesaj trimis, iar fiecare datagramă dintr-un anumit mesaj va avea aceeași valoare în acest câmp de 16 biți.
- **Indicatori** – Acest câmp conține mai mulți biți indicatori. Bitul 0 este rezervat și ar trebui să aibă mereu valoarea 0. Bitul 1 este câmpul *Fără fragmentare* (*Don't Fragment, sau DF*): 0 = se acceptă fragmentarea, 1 = nu se acceptă fragmentarea. Dacă un calculator determină că trebuie să fragmenteze o datagramă pentru a o trimite prin următorul segment din rețeaua fizică și dacă acest câmp DF are stabilită valoarea 1, renunță la datagramă. Dacă acest câmp are valoarea 0, împarte datagrama în mai multe datagramă astfel încât acestea să poată fi trimise mai departe pe traseu. Bitul 2 se numește *Mai multe fragmente* (*More Fragments, sau MF*) și este utilizat pentru a indica starea de fragmentare a pachetului. Dacă are stabilită valoarea 1, trebuie să mai sosească și alte fragmente. Ultimul fragment din mesajul original care a fost fragmentat are valoarea 0 în acest câmp. Împreună, cele două câmpuri controlează procesul de fragmentare.
- **Deplasamentul de fragment** – Atunci când indicatorul MF are stabilită valoarea 1 (adică mesajul a fost fragmentat), acest câmp este folosit pentru a indica poziția fragmentului în cadrul mesajului original astfel încât acesta să poată fi reasamblat corect. Acest câmp are o lungime de 13 biți și exprimă valoarea deplasamentului acestui fragment în unități de 8 octeți.
- **Durata de viață (Time to Live, sau TTL)** – Acest câmp specifică perioada maximă (în secunde) în care i se permite unei datagramă să existe în rețea. Valoarea este stabilită la început și este redusă de fiecare mașină prin care trece datagrama. Când acest câmp ajunge la valoarea 0, se renunță la datagramă. Rețineți că, deși acest câmp poate fi redus cu câteva secunde pe o mașină cu încărcare foarte mare, este redus întotdeauna cu cel puțin o secundă pe fiecare mașină prin care trece, chiar dacă a fost necesară o perioadă mai mică de o secundă pentru prelucrarea datagramelor.
- **Protocolul** – Acest câmp de 8 biți indică tipul de protocol pentru datele conținute în această datagramă. Network Information Center (NIC) stabilește numerele folosite în acest câmp pentru identificarea protocoalelor. De exemplu, TCP este indicat prin plasarea valorii 6 în acest câmp.
- **Suma de control a antetului** – Este o valoare calculată pe 16 biți, utilizată pentru a verifica integritatea informațiilor din antet. Când informațiile din antet sunt modificate, această valoare este recalculată. De exemplu, deoarece valoarea TTL este scăzută de fiecare sistem prin care trece datagrama, se modifică și valoarea sumei de control.
- **Adresa sursă** – Este adresa IP a sursei datagramelor. Acest câmp are lungimea de 32 de biți.
- **Adresa destinație** – Este adresa IP a destinației datagramelor. Acest câmp are lungimea de 32 de biți.

- **Opțiuni** – Acesta este un câmp opțional, de lungime variabilă, care poate conține o listă de opțiuni. Între clasele de opțiuni se numără: control, rezervat, depanare și măsură. *Rutarea la sursă* poate fi implementată cu ajutorul acestui câmp și are o importanță deosebită la configurarea unui firewall.
- **Completare** – Acest câmp este utilizat pentru a completa antetul până la limita de 32 de biți. Completarea se face cu zerouri.

Informații importante din antetul pachetului

Filtrele de pachete operează pe baza informațiilor găsite în antetul IP. Între câmpurile importante se numără adresele sursă și destinație, tipul de protocol și indicatorii de fragmentare. De exemplu, *falsificarea IP* se petrece atunci când un hacker plasează într-un antet de pachet o adresă sursă care nu este sursa reală a pachetului. Din acest motiv, trebuie să vă asigurați atunci când configurați un filtru de pachete că acesta va refuza orice pachet care ajunge la interfața de rețea externă și are o adresă de sursă care indică faptul că pachetul vine din rețeaua internă. Deoarece acest pachet ajunge pe interfața externă, nu poate fi un pachet valid din rețeaua dumneavoastră, ci o încercare a unui hacker de plasare în rețea a unor pachete care arată ca și cum ar fi emise de aici.

Câmpul de opțiuni și rutarea la sursă

Deși câmpul de opțiuni este opțional, poate fi utilizat în moduri pe care ar trebui să le cunoașteți atunci când construiți un firewall. Aici este locul în care se definește *rutarea la sursă* pentru o datagramă. Atunci când am discutat prima dată despre protocolul IP în acest capitol, am spus că IP lasă deciziile de rutare în seama celorlalte protocoale. În majoritatea cazurilor, așa se întâmplă. Însă, după cum puteți vedea în tabelul 2.6, există două opțiuni care pot fi utilizate de IP pentru rutare. Acestea sunt *rutarea liberă la sursă* (opțiunea 3) și *rutarea strictă la sursă* (opțiunea 9).

Tabelul 2.6 Clasele și numerele de opțiuni

Clasă de opțiune	Număr de opțiune	Utilizare
0	0	Indică finalul unei liste de opțiuni
0	1	Fără opțiuni
0	2	Opțiuni de securitate pentru domeniul militar
0	3	Rutare liberă la sursă
0	7	Activează rutarea la sursă
0	9	Rutarea strictă la sursă
2	4	Marca de timp activă

Rutarea la sursă poate fi utilizată de un hacker pentru a forța un pachet să revină la calculatorul său folosind o anumită rută.

Ambele opțiuni oferă o listă de adrese prin care datagrama trebuie să treacă. În cazul rutării libere la sursă, lista trebuie să fie respectată, însă pot fi folosite și alte rute pentru a ajunge la fiecare mașină adresată în listă. În cazul rutării stricte la sursă, lista trebuie respectată cu exactitate, iar în cazul nerespectării, datagrama este respinsă.

Vezi și

- În *capitolul 3*, „Securitate și Internet”, *puteți găsi mai multe informații despre rutarea la sursă și motivele pentru care ar trebui să o dezactivați la nivelul firewall-ului.*

Ce sunt porturile TCP și UDP?

Dacă toate aplicațiile care folosesc rețeaua și-ar identifica destinația pentru transferul de date pe baza unei singure adrese IP, informațiile ar ajunge la calculatorul destinație, însă ar fi aproape imposibil pentru acel sistem să determine cărui proces să-i atribuie datele respective.

Atât protocolul TCP cât și protocolul UDP folosesc numere de porturi pentru a rezolva această problemă. Fiecare aplicație care comunică în rețea folosind TCP/IP specifică și un număr de *port* de pe calculatorul destinație. Numerele de porturi sunt *punctele finale (endpoint)* pentru calea de comunicație, astfel încât două aplicații care comunică prin rețea să se poată identifica una pe cealaltă. Gândiți-vă la adresa unei firme. Dacă toată corespondența ar fi expediată doar cu adresa străzii, cum ați putea determina cine trebuie să preia fiecare scrisoare în parte? Folosind numele unei persoane sau numărul de cameră, punctul final al comunicației este definit mai precis. Acesta este modul în care operează porturile.

Porturi general cunoscute

Internet Assigned Numbers Authority (IANA) este organizația care controlează primul domeniu de numere de porturi disponibile (0-1023), iar acestea sunt numite în mod uzual *porturi general cunoscute (well-known ports)*. Utilizarea acestor porturi a fost definită în câteva documente RFC (cel mai recent în RFC 1700) și se modifică doar ocazional.

Vezi și

- *Veți găsi o listă cu aceste porturi și o scurtă descriere a modului lor de utilizare în tabelul A.1 din anexa A, la pagina 318.*

Porturile general cunoscute sunt de obicei accesibile pe un anumit sistem unui proces privilegiat sau utilizatorilor privilegiați.

De exemplu, puteți vedea că utilitarul Telnet folosește portul 23. În tabelul din anexa A, observați că, în majoritatea cazurilor, User Datagram Protocol (UDP) și Transmission Control Protocol (TCP) utilizează un anumit port în același mod. Însă acest lucru nu este obligatoriu, astfel că atunci când utilizați acest tabel, nu uitați să verificați protocolul pentru fiecare port atunci când îi căutați utilitatea.

Acest tabel poate fi utilizat foarte bine pentru a vă ajuta să vă decideți ce porturi să blocați atunci când construiți un firewall. Unele dintre aceste aplicații nu vor fi utilizate niciodată

de sistemul dumneavoastră, deci nu există nici un motiv să permiteți prin firewall un trafic de rețea care utilizează aceste porturi.

Porturi înregistrate

Pot fi utilizate și porturile numerotate de la 1024 la 65535, care nu sunt rezervate de organizația IANA. Aceste porturi sunt numite porturi înregistrate și pot fi utilizate de aproape orice proces utilizator din sistem.

Servicii TCP/IP uzuale

Au fost create numeroase servicii pentru a lucra cu suita de protocoale TCP/IP. Pe baza politicii dumneavoastră de securitate, ar trebui să decideți cărora dintre aceste servicii le veți permite să treacă prin firewall și în ce direcție.

Telnet

Telnet este o aplicație care permite unui utilizator de pe un calculator să se conecteze de la distanță la un alt calculator, folosind o interfață bazată pe celule de caractere. Telnet rulează în general peste protocolul TCP, astfel încât o conexiune poate fi stabilită și menținută într-o manieră sigură. În timp ce numeroase aplicații moderne de calculator folosite de utilizatorii finali utilizează o interfață grafică, Telnet este destinat mai ales problemelor de gestionare a sistemelor. Deoarece Telnet a fost implementat pe mai multe sisteme de operare diferite, este posibil, de exemplu, să vă conectați la un calculator UNIX de pe un calculator Windows NT. Însă atunci când utilizați Telnet pentru a vă conecta la un sistem UNIX, trebuie să folosiți comenzi UNIX pentru a executa activități pe sistemul UNIX. Telnet vă oferă pur și simplu o fereastră pe mașina situată la distanță, iar dumneavoastră trebuie să utilizați setul de comenzi al mașinii de la distanță pentru a efectua operațiile dorite.

În general, un server Telnet este configurat să ofere protecție pentru calculatorul gazdă prin utilizarea mecanismelor normale de autentificare ale sistemului de operare. Aceasta înseamnă că, pentru a vă conecta la sistemul situat la distanță, trebuie să știți un nume de utilizator și o parolă valide pe acel sistem.

Ar trebui să devină evident pentru dumneavoastră faptul că trebuie să analizați cu foarte multă atenție dacă este cazul să permiteți trecerea serviciului Telnet prin firewall. Chiar dacă vă gândiți că mecanismele de autentificare de pe sistemul dumneavoastră sunt suficiente pentru a vă proteja, s-ar putea să fie o altă situație atunci când vă conectați rețeaua la Internet și, astfel, să transformați sistemul dumneavoastră într-o potențială țintă a unui atac de oriunde din lume. Hackerii sunt foarte buni în utilizarea programelor de spargere a parolilor și, prin utilizarea de metode automate, pot să detecteze de obicei foarte rapid o schemă simplă de autentificare nume de utilizator/parolă.

Dacă intenționați să permiteți utilizarea serviciului Telnet, luați în considerare utilizarea unei gazde bastion pentru oferirea acestui serviciu și adăugați un nivel suplimentar de

securitate prin întrebarea unei aplicații intermediar care implică un nivel suplimentar de protecție prin parolă.

Vezi și

➤ *Gazdele bastion și modul de configurare a acestora sunt discutate în detaliu în capitolul 6, „Utilizarea unei gazde bastion”, la pagina 112.*

Protocolul FTP (File Transfer Protocol)

Chiar dacă aplicația Telnet poate fi foarte utilă pentru executarea de comenzi pe un sistem situat la distanță, mai există un serviciu util pus la dispoziție de File Transfer Protocol (FTP). Acest utilitar vă permite să transferați fișiere între calculatoare. Nici acest serviciu nu este suficient de bun pentru a-i fi permis să opereze printr-un firewall. Iată câteva argumente pentru această afirmație:

- Utilizând FTP, un hacker poate să descarce programe periculoase pe sistemul dumneavoastră. Dacă o aplicație de tip „cal troian” a fost copiată pe calculatorul dumneavoastră, poate să deschidă alte câteva breșe de securitate și chiar să se ascundă printre utilitățile de sistem obișnuite.
- Dacă hackerul a compromis deja sistemul dumneavoastră „ghicind” un nume de utilizator și o parolă, fișierele disponibile utilizând această identitate pot fi furate de hacker. Datele dumneavoastră sunt la fel de sigure ca metodele de protejare a resurselor puse la dispoziție de sistemul de operare.
- O acțiune cu adevărat dăunătoare din partea unui hacker, care poate fi efectuată prin utilitarul FTP, este de a continua să transfere fișiere de mari dimensiuni pe calculatorul dumneavoastră până la umplerea efectivă a discului. Unele sisteme de operare se blochează dacă are loc un astfel de eveniment pe discul sistemului. Oricum, puteți avea mari dureri de cap atunci când trebuie să curățați discul. Servicii cum ar fi accesul FTP anonim pot fi configurate să utilizeze un alt disc decât discul sistem. Chiar dacă aceasta împiedică blocarea sistemului la umplerea discului, nu împiedică oprirea serviciului de acces FTP anonim datorită acestui eveniment.

La fel ca Telnet, FTP vă solicită în mod obișnuit să folosiți o combinație nume de utilizator/parolă validă pe sistemul situat la distanță. Spre deosebire de Telnet, care obligă hackerul să înțeleagă sistemul la care se conectează, FTP nu presupune utilizarea setului fundamental de comenzi al sistemului de operare. Comenzile FTP, cum ar fi GET și PUT, sunt mai mult decât standardizate, iar dacă sunteți capabil să pătrundeți într-un sistem folosind FTP, există șanse să puteți face aproape orice doriți pe sistemul respectiv.

Accesul FTP anonim este utilizat deseori pentru a permite oricui să transfere fișiere pe și de pe un server configurat special în acest scop. Atunci când vă conectați la un astfel de server, ar trebui să utilizați anonymous pentru numele de utilizator. Mai puteți să folosiți ca parolă adresa de poștă electronică, astfel încât calculatorul gazdă să păstreze o înregistrare cu cei care au vizitat situl. Acesta nu este decât un obicei și nu ar trebui luat în calcul pentru a afla cu exactitate baza de clienți a serverului.

Protocolul TFTP (Trivial File Transfer Protocol)

În mod similar cu FTP, și acest serviciu ar trebui să fie oprit la nivelul firewall-ului. Trivial FTP este utilizat de obicei de dispozitive de rețea, cum ar fi ruterele, pentru a face mai ușoară descărcarea de petice software și de alte coduri pentru dispozitivul respectiv. Spre deosebire de FTP, TFTP nu solicită un nume de utilizator sau o parolă! Dezactivați acest serviciu!

Serviciul DNS (Domain Name Service)

Sistemul de nume de domenii (Domain Name System, sau DNS) a fost creat pentru a centraliza procesul de efectuare a modificărilor la nume de rețea pentru atribuirile de adrese și pentru a automatiza procesul de executare a funcțiilor de traducere. La începutul utilizării rețelei Internet, exista o locație centrală (SRI NIC, la Institutul de Cercetare Stanford, în Menlo Park, California) responsabilă pentru întreținerea fișierului HOSTS care conținea numele fiecărei gazde din Internet, împreună cu adresa corespunzătoare. Administratorii aveau obligația să comunice modificările la centrul SRI NIC, iar aceste modificări erau încorporate periodic în fișier. Desigur, aceasta însemna că fișierul trebuia să fie distribuit ulterior la fiecare gazdă în parte, astfel încât aceasta să poată dispune de versiunea actualizată.

DNS folosește o arhitectură ierarhică distribuită care este repartizată pe numeroase calculatoare din Internet. Un server root păstrează informații despre domeniile de pe nivelurile superioare (cum ar fi .COM, .EDU sau .GOV), iar fiecare domeniu din Internet are un server de nume de domeniu responsabil pentru numele calculatoarelor și adresele utilizate în acel domeniu. Calculatoarele client interoghează serverele DNS atunci când au nevoie să obțină adresa unui nume de gazdă. Dacă serverul DNS local cunoaște adresa, o returnează calculatorului client. Dacă nu cunoaște adresa, trimite interogarea mai departe în lanțul de servere DNS până când este găsit un server DNS care poate rezolva numele, presupunând desigur că este vorba de un nume valid.

Una dintre primele implementări ale sistemului DNS a fost dezvoltată la Berkeley pentru sistemul de operare propriu BSD UNIX (versiunea 4.3). Ca urmare, deseori veți întâlni numele BIND (Berkeley Internet Name Domain) în loc de DNS. În timp, au fost descoperite numeroase breșe de securitate în sistemul BIND. Asigurați-vă că aveți cea mai recentă versiune și că ați respectat recomandările privitoare la securitate pentru a fi la curent cu informații despre noile breșe, astfel încât serviciul DNS să nu devină o intrare secretă în rețeaua dumneavoastră. Mai mult, puteți să implementați serviciul DNS pe un server, astfel încât acesta să nu fie compromis de actualizările din afara rețelei dumneavoastră.

Vezi și

➤ *În capitolul 6, „Utilizarea unei gazde bastion”, la pagina 112, veți găsi o serie de tehnici care pot fi utilizate pentru configurarea sigură a unui calculator care va fi folosit ca o gazdă bastion.*

Înregistrarea de pe cel mai înalt nivel din ierarhia DNS se numește domeniu rădăcină și este reprezentată de caracterul punct (.). Sub acest domeniu rădăcină se află directoarele de pe primul nivel, împărțite în două grupuri: geografice și organizaționale. Domeniile geografice sunt folosite pentru specificarea anumitor țări, cum ar fi .au pentru Australia sau .uk pentru United Kingdom (Marea Britanie). Sub fiecare dintre domeniile geografice,

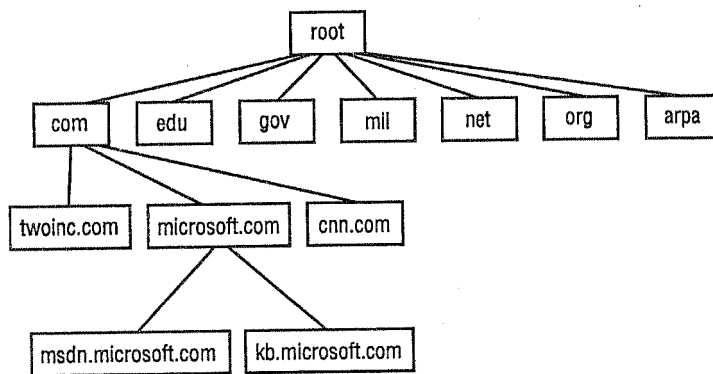
puteți găsi domenii organizaționale. Printre domeniile organizaționale pe care s-ar putea să le cunoașteți se numără următoarele:

- com – Folosit pentru organizații comerciale.
- edu – Folosit pentru organizații educaționale.
- gov – Folosit pentru organizații guvernamentale din Statele Unite.
- mil – Folosit pentru organizații militare din Statele Unite.
- int – Folosit pentru organizații internaționale.
- net – Folosit pentru organizații de rețea, cum ar fi furnizorii de servicii Internet.
- org – Folosit pentru organizații non-profit.
- arpa – Folosit pentru căutări inverse de adrese.

Structura ierarhiei DNS seamănă cu un arbore răsturnat. În figura 2.5 puteți vedea că în vârf se află domeniul rădăcină (root), sub care sunt grupate domeniile de la com la arpa. Sub domeniul com se află organizațiile comerciale individuale care au fiecare un domeniu propriu. Sub fiecare domeniu particular se pot afla diferite subdomenii.

FIGURA 2.5

Domain Name System este o structură distribuită și ierarhică.



La fiecare nivel, un nume complet de domeniu (FQDN, sau fully-qualified domain name) este creat prin concatenarea numelui local cu numele entităților aflate deasupra în ierarhie. Ca urmare, msdn.microsoft.com este folosit pentru denumirea subdomeniului msdn din domeniul Microsoft, de sub domeniul com. Utilizând numele FQDN, este posibilă folosirea multiplă a unui nume de gazdă, cu condiția ca acesta să producă nume FQDN unice. De exemplu, fileserver.twinc.com denumește o gazdă fileserver. Această gazdă nu poate fi confundată cu o altă gazdă cu același nume, dar aflată într-un alt domeniu, cum ar fi fileserver.acme.com.

La stabilirea numelor folosite în sistemul DNS trebuie să fie respectate câteva reguli:

- Lungimea maximă a numelui unui domeniu sau a etichetei unei gazde este de 63 de caractere.
- Lungimea maximă a numelui complet (FQDN) este de 255 de caractere.
- Pot exista cel mult 127 de subdomenii.
- În text nu se face diferențierea între literele mari și cele mici.

Servere de nume principale, secundare și numai pentru cache

Pentru fiecare domeniu din Internet trebuie să existe un server principal și un server secundar. Serverul DNS principal al domeniului conține o colecție de *înregistrări de resurse* (resource records), conținând mapările la adrese ale numelor de gazde din domeniu. Serverul DNS principal ia deciziile finale în privința acestor mapări. Serverul DNS secundar conține o copie a bazei de date întreținută de serverul principal și poate continua rezolvarea numelor atunci când serverul principal este deconectat de la rețea. Este important să rețineți că modificările în baza de date se fac pe serverul DNS principal. Prin folosirea mecanismului de *transfer pe zone*, datele sunt copiate pe serverele secundare.

În multe situații, un server DNS răspunde la interogări de nume din alte domenii decât cel asupra căruia are autoritate. În acest caz, serverul DNS contactează un server DNS aflat pe un nivel superior în ierarhie, până când găsește un server care poate rezolva translatarea numelor sau care poate indica un alt server DNS care are autoritate asupra numelui. Serverul DNS păstrează un cache de nume rezolvate prin această metodă, astfel încât nu este nevoit să interogheze continuu alte servere pentru nume căutate frecvent.

Un al treilea tip de server DNS este serverul numai pentru cache (caching-only server). Acest tip de server nu păstrează o bază de date pentru o anumită zonă. Cu alte cuvinte, nu are autoritate asupra unei zone sau unui domeniu și nu folosește mecanismul de transfer pe zone pentru a păstra o copie curentă a întregii baze de date. Un server de nume numai pentru cache trebuie să ia legătura cu alte servere DNS pentru rezolvarea inițială a unui nume, dar, ca și celelalte servere, păstrează în memoria cache o listă a numelor rezolvate, astfel încât nu este nevoit să retransmită de fiecare dată interogarea către un alt server. Acest tip de server este folosit de obicei într-un segment de rețea conectat cu restul rețelei printr-o legătură mai lentă (sau mai scumpă), pentru a reduce traficul în rețea.

Zone Z1

În multe cazuri, nu este eficient ca un singur server să întrețină baza de date pentru un întreg domeniu. Un server DNS principal poate avea autoritate numai asupra unei zone din domeniu. Zonele sunt formate prin împărțirea domeniului în mai multe subdomenii. De exemplu, un server DNS poate avea autoritate asupra zonei biz.twinc.com, în timp ce un alt server poate avea autoritate asupra zonei research.twinc.com. Ambele subdomenii există în același domeniu: twinc.com. Totuși, prin împărțirea domeniului în subdomenii, devine mai simplă nu numai gestionarea serverelor DNS, ci și a unităților organizaționale sau comerciale individuale deservite de domeniul respectiv.

Un *transfer pe zone* are loc atunci când un server DNS secundar ia legătura cu serverul principal al zonei respective și descoperă că trebuie să obțină modificările efectuate în baza de date. Această decizie este luată pe baza numerelor de serie conținute în baza de date. Dacă serverul secundar are un număr de serie mai mic, este transferată către acesta o nouă copie a bazei de date.

Fișierele din baza de date DNS

Există patru tipuri principale de fișiere folosite de serverele DNS. În cele mai multe implementări DNS, trebuie să folosiți un editor de text pentru efectuarea modificărilor în aceste fișiere. Unele servere DNS mai noi, cum ar fi Microsoft DNS Server, oferă o interfață grafică pentru adăugarea sau modificarea informațiilor în fișierele DNS. Fișierele de bază sunt:

- **Fișierul bazei de date** – Acesta este fișierul în care sunt stocate înregistrările de resurse pentru zonele care intră în responsabilitatea serverului DNS. Prima înregistrare din acest fișier este înregistrarea SOA (Start of Authority).
- **Fișierul de cache** – Acest fișier conține informații referitoare la alte servere de nume ce pot fi folosite pentru rezolvarea interogărilor din afara zonei sau domeniului care intră în responsabilitatea serverului DNS.
- **Fișierul de căutare inversă** – Acest fișier este folosit pentru a furniza un nume de gazdă unui client care nu cunoaște decât adresa IP. Această opțiune este utilă pentru asigurarea securității. De exemplu, un server Web care primește o cerere de la un client poate interoga serverul DNS pentru a verifica dacă numele de gazdă al clientului asociat cu adresa IP este corect.

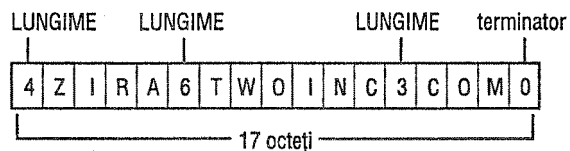
Înregistrări de resurse

De obicei, bazele de date DNS sunt formate din fișiere de text ASCII conținând înregistrări ce pot fi folosite pentru transformarea unui nume într-o adresă IP. Există mai multe tipuri de înregistrări ce pot fi folosite în bazele de date, fiecare reprezentând un anumit tip de resurse, cum ar fi numele de gazdă al unui calculator sau numele unui server de poștă electronică.

Pentru reprezentarea unui nume de domeniu în DNS este folosită o sintaxă specifică. Pentru descrierea acestei sintaxe, în documentul RFC 1035, „Nume de domenii – implementare și specificații”¹ este folosit termenul „etichetă” (label). O etichetă este formată dintr-un câmp de lungime (length field) cu dimensiunea de un octet, urmat de un câmp de date. Câmpul de lungime indică numărul de caractere din câmpul de date. Numele unui domeniu este reprezentat printr-o serie de etichete și întregul șir ce formează numele domeniului se termină cu un câmp de lungime cu valoarea zero. De exemplu, figura 2.6 prezintă organizarea unei serii de etichete folosite pentru definirea domeniului cu numele zira.twoinc.com.

FIGURA 2.6

DNS folosește o serie de etichete pentru a reprezenta un nume unui domeniu.



Deși șirul de caractere are numai 13 caractere, excluzând punctele, este reprezentat în baza de date pe 17 octeți, din cauza câmpurilor de lungime și a terminatorului. Pentru a evita

¹ În original, „Domain Names – Implementation and Specification” (n.trad.)

repetarea numelor de domenii folosite frecvent în baza de date, poate fi utilizată o înregistrare pointer.

Formatul general folosit pentru înregistrările de resurse conține următoarele câmpuri:

- **Name (Nume)** – Numele proprietarului. Acesta este numele domeniului căruia îi aparține înregistrarea.
- **Type (Tip)** – Un câmp de doi octeți care precizează codul de tip al înregistrării de resurse.
- **Class (Clasă)** – Un câmp de doi octeți care precizează codul de clasă al înregistrării de resurse.
- **TTL** – Un întreg cu semn pe 32 de biți care specifică durata de viață (time-to-live, sau TTL). Valoarea TTL specifică perioada în care poate fi păstrată o înregistrare în cache înainte de a fi reîmprospătată de la sursa care deține autoritatea în zona respectivă. O valoare zero arată că înregistrarea respectivă nu poate fi păstrată în cache.
- **RDLLENGTH** – Un întreg fără semn pe 16 biți, indicând lungimea câmpului de date care urmează.
- **RDATA** – Câmpul de date. Această parte a înregistrării descrie resursa. Conținutul câmpului depinde de valorile câmpurilor Type și Class.

Câmpul Type indică tipul înregistrării de resurse. Tabelul 2.7 conține o listă a tipurilor de înregistrări, împreună cu o descriere a modului de folosire a acestora.

Tabelul 2.7 Înregistrări de resurse DNS

Tipul înregistrării	Descriere
A	Adresa IP a gazdei
AAAA	Adresa IP a gazdei (IPv6)
NS	Înregistrarea serverului de nume (Name Server Record)
PTR	Pointer către o altă înregistrare de nume de domeniu
SOA	Începutul zonei de autoritate
WKS	Serviciu general cunoscut (Well-Known Service)
HINFO	Informații despre gazde
MX	„Mail Exchanger” pentru domeniu
MINFO	Informații despre căsuța poștală sau lista poștală
TXT	Înregistrare de tip text pentru informații diverse
CNAME	Nume canonic pentru alias

În primele implementări ale serviciului DNS erau folosite și alte tipuri de înregistrări. De exemplu, tipurile MD și MF erau utilizate pentru specificarea înregistrărilor Mail Destination (destinație de poștă electronică) și Mail Forwarder (retransmiterea mesajelor de poștă electronică). Documentul RFC 1035 a abrogat alte trei specificații RFC: 882, 883 și 973. Există alte patru tipuri, considerate experimentale:

- **MB** – Nume de domeniu pentru căsuța poștală electronică
- **MG** – Membru al unui grup de poștă electronică
- **MR** – Numele de domeniu de redenumire în poșta electronică
- **NULL** – Înregistrare de resursă vidă

Înregistrarea SOA (Start of Authority) este folosită la începutul bazei de date pentru descrierea acesteia. Este folosită în principal de serverele DNS secundare pentru a obține informații despre zone. Câmpurile acestei înregistrări sunt:

- **Numele domeniului** – Numele domeniului în care își exercită autoritatea această bază de date.
- **IN** – Tipul de clasă pentru Internet.
- **SOA** – Indicator de tip pentru înregistrarea Start of Authority.
- **Server primar** – Numele FQDN al serverului DNS primar pentru acest domeniu.
- **Adresă de poștă electronică** – Adresa de e-mail a persoanei care are în responsabilitate acest domeniu.
- **Număr de serie** – O valoare pe 32 de biți care specifică numărul de revizuire al fișierului bazei de date. Este incrementat de fiecare dată când se face o modificare în baza de date, astfel încât serverele secundare să poată detecta această schimbare.
- **Frecvența de reîmprospătare** – O valoare pe 32 de biți utilizată de serverele secundare. După trecerea acestui interval de timp, datele unei înregistrări trebuie verificate din nou în baza de date a serverului primar.
- **Frecvența de repetare a încercărilor** – O valoare pe 32 de biți, indicând perioada de așteptare înainte de a încerca din nou reîmprospătarea datelor, după o încercare nereușită.
- **Durata de expirare** – O valoare pe 32 de biți, indicând intervalul maxim de timp în care un server secundar ar trebui să încerce reîmprospătarea datelor înainte de a înceta să mai prelucreze datele DNS pentru această zonă.
- **Valoarea TTL minimă** – Durata minimă de viață a unei înregistrări de resursă. Această valoare poate fi suprascrisă de valoarea TTL specificată chiar în înregistrare.

Toate valorile pentru durate din înregistrarea SOA sunt specificate în secunde.

Tipul de înregistrare NS poate fi folosit pentru a preciza că un alt server de nume are autoritate asupra acestui subdomeniu. De exemplu, următoarea înregistrare arată că serverul de nume al cărui nume de gazdă FQDN este zira.twoinc.com este autoritatea de la care pot fi obținute informații despre subdomeniul zork.twoinc.com:

```
zork.twoinc.com IN NS zira.twoinc.com
```

Pentru a obține adresa serverului de nume zira.twoinc.com, este necesară o înregistrare de tip „A”:

```
zira.twoinc.com IN A 216.65.33.219
```

Înregistrările CNAME sunt folosite pentru specificarea pseudonimelor¹ ce pot fi utilizate împreună cu numele de gazdă, ca în exemplul următor:

```
ftp.zira.twoinc.com IN CNAME zira.twoinc.com
```

¹ În original, *alias* sau *nickname* (n. trad.)

Înregistrările de tip pointer (clasa PTR) sunt folosite pentru obținerea numelui asociat cu o adresă IP – o traducere inversă. De exemplu, înregistrarea următoare poate fi folosită de o interogare pentru obținerea numelui acestei gazde atunci când este cunoscută numai adresa IP:

```
219.33.65.216 IN PTR zira.twoinc.com
```

Remarcați, totuși, că adresa IP a fost inversată. Într-o înregistrare de tip pointer, adresa IP este reprezentată sub forma 219.33.65.216 în loc de 216.65.33.219. Formatul inversat este folosit pentru a permite funcționarea corespunzătoare a procedurii de căutare după cheie în baza de date. Domeniul special este numit IN-ADDR.ARPA. Aceste date sunt folosite atunci când un server trebuie să caute în baza de date un nume de gazdă corespunzător unei adrese din domeniu.

În general, câmpul Class are valoarea IN, prescurtarea de la Internet. Valoarea numerică a acestui cod este 1. Pe lângă acest tip de clasă, puteți întâlni valoarea CS, care este prescurtarea de la vechea clasă CSNET. Codul CH este prescurtarea clasei CHAOS, iar codul HS este prescurtarea de la clasa Hesiod.

Protocolul SMTP (Simple Mail Transfer Protocol)

Acest protocol reprezintă baza pentru toate mesajele de poștă electronică pe care le trimiteți prin Internet. Dintre toate serviciile oferite de Internet, acesta este unul dintre cele mai utilizate și, de asemenea, unul dintre cele mai des atacate. Programele inițiale utilizate pentru SMTP erau foarte mari și complexe, astfel că aveau numeroase probleme de securitate. Una dintre cele mai evidente probleme este capacitatea de a falsifica adresa expeditorului. Dacă un hacker vă poate face să deschideți un fișier atașat unui mesaj de poștă electronică doar pentru că aveți impresia că știți expeditorul și aveți încredere în acesta, puteți să introduceți în sistemul dumneavoastră un virus sau un alt program generator de probleme.

Vezi și

- În capitolul 6, „Utilizarea unei gazde bastion”, la pagina 131, veți găsi câteva metode care pot fi utilizate pentru a implementa într-un mod sigur un sistem de poștă electronică Internet pentru rețeaua dumneavoastră, cu riscuri minime.

Atâta vreme cât există viruși de calculator și alte programe dăunătoare, nu veți putea să rezolvați aceste probleme folosind un firewall. Dacă doriți să aveți un sistem de poștă electronică în rețea cu acces din exterior, trebuie să vă luați măsuri de prevedere suplimentare. Ar trebui să utilizați un program bun, actualizat regulat de producător, pentru a căuta, a identifica și a distruge aceste tipuri de programe.

Utilitățile r

Serviciile Berkeley r au fost proiectate pentru a simplifica o serie de activități executate în mod obișnuit într-o rețea. Ele sunt denumite utilitare r deoarece fiecare utilitar din această categorie este folosit pentru acțiuni de la distanță și numele fiecăruia începe cu cuvântul „remote”. Utilitățile r de bază sunt următoarele:

- **rlogin** Similar cu Telnet, însă mai puțin complex, acest utilitar vă permite să vă conectați la un sistem situat la distanță și să îi utilizați setul de comenzi pentru a efectua activități ca și cum v-ați afla în fața acelui calculator.
- **rsh** Acest utilitar vă permite să executați comenzi pe un sistem aflat la distanță.
- **rcp** Acest utilitar este similar cu FTP prin faptul că poate fi utilizat pentru a copia fișiere între sistemele dintr-o rețea.
- **rwho** Acest utilitar rulează ca un proces demon pe un sistem situat la distanță pentru a aduna informații despre utilizatorii din rețeaua de la distanță.
- **ruptime** Acest utilitar afișează o listă de calculatoare din rețeaua aflată la distanță și informații despre acestea, cum ar fi numărul de utilizatori și perioada de funcționare a sistemului de la pornire.
- **rexec** Acesta este un utilitar mai vechi și poate fi utilizat pentru a executa comenzi pe un sistem situat la distanță.

Numele acestor comenzi vă sugerează că ele sunt utile, nu-i așa? Cu toate acestea, ele pot fi foarte periculoase nu numai când sunt utilizate printr-un firewall, ci chiar atunci când sunt utilizate în rețeaua dumneavoastră locală. Aceasta se datorează în principal metodei folosite pentru autentificarea utilizatorului aflat la distanță care întrebuițează utilitarul `r`.

Utilizatorul nu trebuie să specifice un nume de utilizator sau o parolă atunci când folosește un utilitar `r`. Pe sistemul situat la distanță există două fișiere care pot fi utilizate pentru a permite accesul la sistem. Acestea sunt fișierele `host.equiv` și `.rhosts`.

Fișierul `host.equiv` conține o listă de sisteme aflate la distanță cărora li se va permite accesul pe acel calculator. Administratorul de sistem răspunde de întreținerea acestui fișier, la fel cum procedează cu fișierul de parole. Prin plasarea în acest fișier doar a numelor de gazdă, corespunzătoare unor sisteme sigure, ați putea crede că sunteți protejat. Însă ar trebui să luați în calcul ceea ce poate rezulta cu adevărat de aici. Prin plasarea numelui unui sistem situat la distanță în acest fișier, deveniți vulnerabil la un atac în cazul în care oricare dintre acele sisteme aflate la distanță ar fi compromis! Dacă un hacker pătrunde într-un anumit calculator, el va avea acces la toate celelalte sisteme în care acest calculator are încredere prin fișierul `host.equiv`!

Din nefericire, poate fi și mai rău. Fișierul `.rhosts` nu se află sub controlul administratorului de sistem. Acest fișier se găsește în directorul de bază al unui utilizator și, la fel ca fișierul `host.equiv`, conține numele unor sisteme sigure, situate la distanță. În acest fișier `.rhosts`, numele de sistem este urmat de numele de utilizatori, și numai acelor utilizatori le este permis accesul – același tip de acces pe care utilizatorul îl are pe sistemul local.

După cum puteți vedea, nu este nevoie decât de un utilizator needucat (sau supărat) pentru a crea o breșă de securitate în sistemul dumneavoastră.

Nu folosiți utilitățile `r` prin firewall. Dezactivați-le. Dacă veți permite utilizarea lor în rețeaua locală, ar trebui să verificați regulat fișierele `host.equiv` și `.rhosts` pentru a vă asigura că nu sunt folosite în mod abuziv.

Alte servicii de rețea

Acest capitol nu a prezentat decât serviciile TCP/IP de bază, care există și sunt utilizate de mai mult timp. Însă sunt dezvoltate și alte protocoale și servicii și veți remarca zilnic noutăți în această privință. De exemplu, World Wide Web utilizează protocolul HTTP pentru a transfera pagini Web către browserul dumneavoastră. RealAudio este un serviciu care poate permite calculatorului dumneavoastră să funcționeze ca un telefon sau ca un aparat de radio. Nu este scopul acestei cărți să detalieze sutele de servicii disponibile. Trebuie accentuat din nou faptul că atunci când proiectați firewall-ul, ar trebui să dezactivați toate serviciile și protocoalele și apoi să le activați doar pe cele de care aveți nevoie. Aceasta vă va ajuta să vă protejați împotriva noilor protocoale și servicii.

Rezumat

Înainte de a începe să înțelegeți modul în care un firewall vă protejează rețeaua, indiferent dacă este vorba de un filtru de pachete sau de un server intermediar, trebuie să înțelegeți foarte bine modul de funcționare a suitei TCP/IP și a serviciilor pe care le poate oferi. Atunci când utilizatorii vă spun că au nevoie de un serviciu sau altul, sau că trebuie să folosească un anumit protocol, ar trebui să fiți capabil să discutați cu ei într-o manieră rațională și să vă apărați politica de firewall. Dacă este necesar, puteți să utilizați oricând un calculator independent cu conexiune proprie la Internet pentru a pune la dispoziție servicii cu adevărat periculoase. În capitolele următoare, veți studia câteva dintre problemele de securitate pe care le pot provoca unele protocoale și servicii. De asemenea, veți analiza câteva metode de implementare a unui firewall pentru a face ca utilizarea acestora să fie ceva mai sigură.

Capitolul 3

Securitate și Internet

- Rețele LAN și WAN
- Securitatea într-o rețea locală de calculatoare
- Securitatea într-o rețea de mare suprafață

Rețele LAN și WAN

Cea mai mare diferență dintre securitatea într-o rețea locală de calculatoare și între-o rețea de mare suprafață, cum ar fi Internet, este controlul. Într-o rețea LAN, administratorul de rețea (și posibil unii administratori de sistem) poate să exercite un control foarte bun asupra calculatoarelor gazdă din rețea și asupra operațiilor și gestionării rețelei. Atunci când o rețea locală este conectată la Internet, deveniți parte a unei interconexiuni mult mai mari de rețele asupra cărora aveți foarte puțin control sau chiar deloc. Datorită acestui fapt, problemele de securitate care pot fi întâlnite într-o rețea LAN obișnuită sunt minore în comparație cu cele care pot apărea din Internet.

Un motiv este numărul imens de calculatoare care fac parte din Internet. Acum nu mai este nevoie ca un infractor să intre în camera calculatorului și apoi în calculator. Nu mai este necesar ca un hacker să încerce în mod repetat să pătrundă în rețeaua dumneavoastră trecând peste securitatea modemului. În Internet, un atacator poate să vină practic din orice parte a globului pentru a încerca aceste șmecherii.

Securitatea într-o rețea locală de calculatoare

Într-o rețea locală, știți ce protocoale sunt utilizate și puteți să configurați monitorizarea și auditarea astfel încât să urmăriți abuzurile. Chiar și într-o rețea mare de companie, instrumentele bazate pe protocolul SNMP (Simple Network Management Protocol) sau RMON oferă un control centralizat și urmăresc securitatea.

Ce este RMON?

RMON este acronimul expresiei Remote Monitoring (Monitorizare de la distanță). RMON este un instrument de colectare și analiză a datelor, util pentru monitorizarea de la distanță a componentelor rețelei, cum ar fi calculatoare, rutere, comutatoare și alte dispozitive de rețea. Funcționalitatea instrumentului RMON, care este descris în documentele RFC 1513 și 1757, extinde capabilitățile de monitorizare puse la dispoziție de protocolul SNMP.

Autentificarea utilizatorilor

Forma de bază de securitate folosită într-o rețea locală de calculatoare este contul și parola de utilizator. Când această metodă este implementată într-un mod sigur, fiecare utilizator care accesează rețeaua are un nume de cont unic (sau nume de utilizator), atribuit de administratorul de rețea, și o parolă care în mod uzual se află sub propriul control. Această formă de autentificare provine de la primele calculatoare independente (care nu erau legate în rețea) pe care rulau sisteme de operare multiutilizator. Numele de utilizator unic permitea sistemului de operare să țină evidența utilizatorilor conectați la calculator, ceea ce făcea posibilă acordarea de drepturi și privilegii diferite utilizatorilor, în funcție de nevoile fiecăruia. Administratorul care crea contul de utilizator crea și o parolă inițială. Însă era responsabilitatea utilizatorului să schimbe acea parolă inițială cu o expresie greu de descoperit. De asemenea, era responsabilitatea utilizatorului să protejeze parola astfel încât să nu fie cunoscută de nimeni altcineva.

Când acest tip de autentificare este integrat în tehnologiile rețelelor locale de calculatoare, poate deveni puțin mai complicat. Când este vorba de un singur calculator, este ușor de întreținut o singură bază de date sigură, care memorează numele de utilizatori și parolele pe care sistemul de operare le poate utiliza pentru a verifica utilizatorii. Când sunt legate în rețea mai multe calculatoare, unde sunt plasate aceste informații de securitate?

În unele sisteme de operare, cum ar fi UNIX, fiecare calculator din rețea are propria bază de date cu parole – fișierul `/etc/passwd`. Acest fișier memorează numele de utilizatori și parolele, împreună cu alte informații pertinente despre contul utilizatorului. Cu toate că acest fișier este un simplu fișier text care poate fi tipărit și analizat, rămâne relativ sigur, deoarece parolele stocate în fișier sunt criptate. Aceasta înseamnă că sistemul este sigur dacă aveți încredere în utilizatorii din rețeaua dumneavoastră. Programe cum ar fi Crack pot fi utilizate pentru a descoperi valorile acestor parole criptate, astfel că, după cum probabil deduceți, această metodă de autentificare sigură lasă de dorit atunci când vă conectați la Internet.

Ar trebui să fie evident de la început că această metodă de utilizare a unor baze de date de securitate diferite pentru fiecare calculator din rețea are propriile dezavantaje. De exemplu, o politică bună de securitate spune că utilizatorul trebuie să își schimbe parola după ce aceasta a fost utilizată mai mult timp. Dacă utilizatorul trebuie să acceseze resurse de pe mai multe calculatoare din rețeaua LAN, trebuie să își schimbe parola pe mai multe calculatoare atunci când vine vremea să facă o schimbare.

Utilizarea unui fișier de parole ascuns

O metodă de îmbunătățire a securității parolelor memorate uzual în fișierul `/etc/passwd` este de a folosi un fișier de parole ascuns, care nu poate fi citit de oricine. Studiați documentația versiunii de UNIX cu care lucrați pentru a afla dacă această caracteristică este disponibilă.

Sincronizarea fișierelor de parole

Deși sistemul UNIX are mai multe componente integrate pentru lucrul în rețea, îi lipsește o metodă de sincronizare a fișierelor de parole între mai multe sisteme dintr-o rețea. În domeniile Windows NT, unul sau mai multe servere au rol de controlere de domeniu și controlează conectările utilizatorilor la domeniul respectiv. În UNIX, fiecare server are propriul fișier de parole. Dacă utilizatorii vor să se conecteze la mai multe sisteme din rețea, trebuie să aibă câte un cont pe fiecare sistem. Pentru a rezolva acest dezavantaj, firma Sun a dezvoltat o aplicație denumită Yellow Pages,

care are rolul de a păstra sincronizarea fișierelor importante de sistem. Datorită unei dispute pentru o marcă comercială, Yellow Pages a fost redenumită NIS, acronim de la Network Information Service.

Sistemele de operare în rețea pot oferi o soluție prin utilizarea unei baze de date de conectare în rețea, care conține conturile pentru toți utilizatorii din rețea. În Windows NT, este folosit conceptul de domeniu pentru a grupa utilizatorii într-o bază de date SAM centrală (Security Accounts Manager). Atunci când un utilizator se conectează la un calculator Windows NT care face parte din domeniu, este autentificat printr-un dialog între stația de lucru a utilizatorului și un server care operează ca un controller de domeniu. Primele versiuni ale sistemului de operare Novell NetWare permiteau utilizatorilor să se conecteze la fiecare server pe care îl accesau. În prezent, există serviciul NDS (Novell Directory Services) care pune la dispoziție o bază de date centralizată a utilizatorilor.

Atunci când este realizată o conexiune la Internet, problema autentificării utilizatorilor devine și mai dificilă. Când utilizatorii mobili sunt în afara biroului, ar trebui să folosească un modem pentru a contacta biroul de bază sau pot folosi Internetul? Dacă este folosită rețeaua Internet, cum poate fi asigurată o sesiune sigură de conectare în rețea? Există mai multe soluții la această problemă, de la tehnologia Kerberos și criptarea cu chei publice și până la rețelele private virtuale (VPN).

- *Criptarea și comunicațiile sigure în Internet sunt subiecte importante. Pentru mai multe informații despre aceste subiecte, vezi:*
- *Capitolul 9, „Tehnologii de criptare”, pagina 166*
- *Capitolul 10 „Rețele virtuale private (VPN) și tuneluri”, pagina 175*
- *Capitolul 11, „Utilizarea programului PGP (Pretty Good Privacy) pentru criptare”, pagina 188*

Protejarea resurselor

Autentificarea utilizatorilor este primul lucru la care se gândesc majoritatea dintre noi atunci când este vorba de securitatea calculatoarelor. După ce un utilizator este autentificat pentru un calculator sau o rețea, următorul mecanism folosit pentru controlul accesului este protejarea resurselor. Sistemele UNIX, Windows NT, Novell NetWare, alte sisteme de operare și sisteme de operare în rețea oferă diferite forme de protejare a resurselor, care vă permit să specificați ce fișiere, directoare, imprimante și așa mai departe sunt accesibile pentru utilizatori. Protejarea resurselor poate fi utilizată pentru a restricționa utilizatorii care pot avea acces la obiecte, iar tehnicile de auditare pot fi folosite pentru a urmări modul de utilizare, ca și abuzul de privilegii.

La fel ca bazele de date pentru autentificarea utilizatorilor, administratorii de sisteme și de rețea ai rețelei LAN controlează resursele pe sistemul conectat la rețea. Însă acest control se bazează pe presupunerea că metodele de autentificare a utilizatorilor sunt absolut sigure și că ați configurat corect protejarea resurselor.

Acum știu că metodele simple de autentificare sunt ușor de contrariat, dacă se dispune de timp suficient. Metodele care erau eficiente într-o rețea LAN mică nu sunt suficiente atunci când vă conectați la o rețea mult mai mare. Dacă metodele de autentificare eșuează, protejarea resurselor înseamnă foarte puțin, pentru că un atacator poate să devină aproape orice utilizator dorește.

Protejarea resurselor nu oferă o protecție totală împotriva intrușilor. Printr-o conexiune la Internet, vă expuneți rețeaua la mult mai mulți potențiali intruși decât vă puteți imagina. Pentru a vă proteja resursele de rețea, trebuie luate măsuri suplimentare. Sistemele firewall, care constituie subiectul acestei cărți, reprezintă următoarea etapă importantă.

Dispozitive fizice de siguranță

Când aveți de-a face cu calculatoare conectate într-o rețea locală, este relativ ușor să asigurați securitatea sitului fizic. Ținând sub cheie serverele importante, puteți preveni de obicei compromiterea voită a acestora. Chiar dacă rețeaua locală se întinde în mai multe clădiri, cum este cazul într-un campus studentesc, securitatea fizică este controlabilă local de către o persoană desemnată.

Atunci când rețeaua este conectată la Internet, devine parte a unei rețele mult mai mari, asupra căreia nu aveți nici un control fizic. Ați putea avea o oarecare influență asupra furnizorului ISP pentru a putea controla modul în care este configurat ruterul pentru serviciul dumneavoastră, însă nu aveți nici un control asupra milioanele de calculatoare gazdă, rutere, comutatoare și alte echipamente existente în Internet. Firewall-ul este metoda pe care o utilizați pentru a crea o barieră rezistentă care, sperați dumneavoastră, va ține la distanță persoanele care vor să provoace daune în rețea.

Securitatea într-o rețea de mare suprafață

O conexiune la Internet expune rețeaua locală la un număr infinit de probleme de securitate și potențiali atacatori. Problemele pe care le aveți cu utilizatorii din rețeaua locală sunt mici atunci când sunt comparate cu un atac din partea unei persoane experimentate în tehnicile moderne de „spargere” a rețelelor de calculatoare. Atunci când o rețea este conectată la Internet, există toate motivele pentru îmbunătățirea suplimentară a securității pe calculatoarele gazdă locale. Un firewall bun, care să aibă rolul de punct unic de control pentru conexiunea Internet, este necesar pentru a vă susține apărarea. În următoarele secțiuni, veți analiza câteva dintre tipurile de probleme care pot apărea, astfel încât să înțelegeți mai bine de ce este necesar un firewall și de ce o conexiune la Internet nu trebuie considerată sigură.

Intrările secrete și breșele protocoalelor de rețea

TCP/IP și multe dintre protocoalele și utilitățile care au legătură cu această suită au fost dezvoltate cu mulți ani în urmă, când amenințările de securitate asupra Internetului erau puține în comparație cu problemele din prezent. Ca urmare, cele mai multe dintre aceste protocoale și utilități nu au fost scrise având ca prioritate securitatea. Ele au fost proiectate pentru funcționalitate și portabilitate. Acest concept a ajutat la răspândirea TCP/IP pe numeroase platforme diferite, iar în prezent este suita de protocoale care realizează conectarea la Internet.

Vezi și

- Pentru mai multe informații despre suita TCP/IP și protocoalele și utilitățile care au legătură cu aceasta, vezi capitolul 2, „Introducere în suita de protocoale TCP/IP”, la pagina 26.

S-a constatat că o parte dintre utilitățile create au erori semnificative de programare, care puteau fi utilizate de persoane hotărâte să facă rău. De exemplu, aplicația sendmail a fost folosită abuziv de foarte multe ori și, de-a lungul anilor, a provocat dureri de cap administratorilor de rețea. Uneori, un proiect simplu de program poate determina blocarea unei aplicații într-un mod pe care proiectantul nu l-a anticipat. Bufferele de memorie se pot dovedi prea mici, iar dacă programul nu detectează eroarea neașteptată, aplicațiile s-ar putea bloca sau s-ar putea comporta într-un mod neobișnuit. O astfel de eroare de programare devine o problemă de securitate în cazul în care un hacker o descoperă și o folosește pentru a obține privilegiile sau acces într-o zonă interzisă.

Din nefericire, va mai trece mult timp până când calculatoarele vor fi proiectate astfel încât să poată detecta toate greșelile pe care le poate face un om, așa că vă puteți aștepta să vedeți programe noi care dispar de pe piață la câteva luni de la lansare, după descoperirea unor erori de programare. Uneori este recomandat să rămâneți puțin în urma tehnologiei de ultimă oră pentru a vedea ce se întâmplă.

Actualizați permanent peticele și sfaturile de securitate de la furnizori pentru sistemele de operare și aplicațiile pe care le utilizați.

Vezi și

- Actualizarea periodică a sfaturilor de securitate nu este atât de dificilă pe cât pare. Există câteva situri Web bune care conțin documente ce descriu noile probleme de securitate pe măsură ce sunt descoperite și în multe cazuri, proceduri, petice sau alte soluții care vă pot ajuta să vă apărați împotriva acestor probleme. Consultați anexa C, „Resurse suplimentare”, pentru o listă de situri Web și liste postale care au legătură cu problemele de securitate.

Ce este rutarea la sursă și de ce nu este o soluție bună?

Protocolul IP este un protocol fără conexiune, nefiabil. În majoritatea cazurilor, singurele informații despre destinația unui pachet, disponibile protocolului IP, sunt adresele sursei și destinației conținute în antetul IP. Alte protocoale de rutare implementează mecanismele de decizie a căii pe care o va parcurge un pachet prin Internet pentru a ajunge la destinația finală. În capitolul 2, „Introducere în suita de protocoale TCP/IP”, au fost analizate câmpurile din antetul IP. Vă veți aminti de câmpul Options, care poate fi utilizat pentru a specifica o rută pe care ar trebui să circule pachetul. Această tehnică se numește *rutarea la sursă* (source routing) și a fost dezvoltată pentru utilizări de genul depanării problemelor de rețea și alte activități de mentenanță. Această caracteristică poate fi exploatată cu ușurință de un hacker pentru a introduce în rețeaua dumneavoastră un pachet care pare că a fost generat acolo. Pachetul conține o adresă IP falsificată, dar validă în rețeaua dumneavoastră. Opțiunile de rutare la sursă sunt utilizate pentru a specifica o cale pe care ar trebui să circule pachetul pentru a ajunge la destinație.

Sistemele firewall ar trebui configurate pentru a respinge toate pachetele care au activată opțiunea de rutare la sursă.

Atacuri de tip interzicerea serviciului

Nu toți hackerii plănuiesc să pătrundă în rețeaua dumneavoastră pentru a fura informații. Unii nu vor decât să vă bată la cap. Un atac de tip interzicerea serviciului este un termen general pentru numeroasele metode care pot fi utilizate pentru a vă împiedica să folosiți parțial sau complet rețeaua. Scopul atacatorului este de obicei unul dintre următoarele:

- Supraîncărcarea unei resurse limitate
- Blocarea/căderea unui dispozitiv de rețea sau calculator gazdă
- Reconfigurarea unei resurse pentru a o face inutilă

Supraîncărcarea unei resurse limitate poate să se manifeste în mai multe feluri. Un mod simplu de manifestare este umplerea unui hard-disc astfel încât nimeni să nu mai poată să îl utilizeze. Din acest motiv ar trebui să monitorizați foarte atent orice stocare pe disc alocată unui serviciu FTP anonim ce permite utilizatorilor să încarce fișiere. Evident, nu trebuie să plasați rădăcina (root) unui serviciu FTP pe același disc pe care plasați un sistem de operare. În mod asemănător, nu ar trebui să o plasați nici pe un disc utilizat de o altă aplicație sau de un serviciu care poate avea de suferit în urma unui astfel de atac.

Între alte resurse valoroase se numără memoria, lărgimea de bandă de rețea și timpul de CPU. Resursele nu trebuie să fie neapărat componente fizice ale calculatorului gazdă. Atacul de tip inundarea SYN lucrează prin umplerea cozii pe care TCP/IP o folosește pentru a păstra cererile de conectare sosite pentru un anumit port. Chiar dacă există multă memorie disponibilă în calculator și care poate fi utilizată, acest aspect nu are importanță deoarece coada însăși este limitată de modul în care a fost implementată stiva TCP/IP pentru un anumit sistem de calcul.

Blocarea unui calculator gazdă îl împiedică evident să satisfacă cererile clienților. Unele atacuri de acest tip obțin aceste rezultate prin exploatarea erorilor de programare din sistemul de operare sau din serviciile de rețea. Uneori, nu trebuie decât să fie blocată aplicația care oferă servicii de rețea.

Reconfigurarea unui calculator gazdă poate să aibă loc după ce un intrus a pătruns în rețeaua dumneavoastră și a putut să modifice sistemul de operare sau fișierele de configurare ale aplicației. De aceea este atât de important ca sistemele de calcul pe care le utilizați pentru a pune la dispoziție servicii de rețea să fie protejate total utilizând mecanismele oferite de sistemul de operare.

Vezi și

- Capitolul 6, „Utilizarea unei gazde bastion”, de la pagina 112, și capitolul 8, „Tehnici de monitorizare și auditare a sistemelor de operare”, de la pagina 148, vă pot asista în configurarea unui calculator gazdă protejat.

De asemenea, este posibil să fie reconfigurate și informațiile de rețea, cum ar fi tabelele de rutare, prin utilizarea protocolului ICMP. Acest tip de atac poate face ca un calculator gazdă să pară de negăsit, deși în realitate acesta este funcțional în cadrul rețelei. Dacă tabelul de rutare al ruterului nu conține informații corecte despre modul în care trebuie atinsă o destinație dată, nu contează dacă nodul destinație este pornit sau oprit, deoarece oricum traficul nu va ajunge la el.

Problema cu încercarea de a vă proteja împotriva unui atac de tip interzicerea serviciului este că nu aveți control decât în cadrul rețelei proprii și nu în întreaga rețea Internet. Unele atacuri pot fi oprite de către firewall.

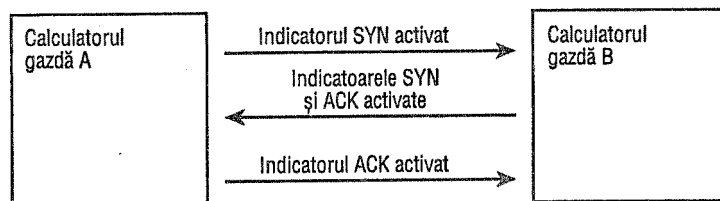
Inundarea SYN

Protocolul TCP este orientat spre conexiune și folosește o metodă de contactare în trei etape pentru a configura o conexiune înainte să aibă loc transferul efectiv al datelor. Antetul TCP folosește câteva câmpuri pentru a configura și gestiona conexiunea. Câmpul pentru numărul de secvență (Sequence Number) este utilizat pentru a ține evidența ordinii pachetelor transmise. Câmpul SYN Flag este utilizat pentru a începe o solicitare de conexiune. Câmpul ACK Flag este utilizat pentru a confirma un pachet. Câmpul FIN Flag este utilizat pentru a termina o conexiune după ce expeditorul a încheiat transmisia.

Metoda de contactare în trei etape folosită pentru a configura o conexiune este un simplu schimb de pachete, după cum puteți vedea în figura 3.1.

FIGURA 3.1

Pentru configurarea unei conexiuni TCP este folosit un dialog de confirmare în trei etape.



Secvența de evenimente este următoarea:

- Calculatorul gazdă A trimite un pachet către Calculatorul gazdă B având bitul SYN activat (configurat la valoarea 1). Câmpul Sequence Number este setat la numărul de secvență inițial care va fi utilizat de Calculatorul gazdă A.
- Calculatorul gazdă B configurează în memorie câteva structuri de date care vor fi utilizate pentru gestionarea conexiunii și apoi răspunde la solicitarea de conexiune trimițând un pachet către Calculatorul gazdă A având câmpul ACK setat la valoarea 1 pentru a confirma primirea pachetului expediat de Calculatorul gazdă A. Al doilea pachet din dialogul de confirmare are de asemenea bitul SYN setat la valoarea 1, comunicând astfel Calculatorului gazdă A că în câmpul Sequence Number al acestui pachet este conținut numărul de secvență inițial al Calculatorului gazdă B.
- În final, când Calculatorul gazdă A recepționează o confirmare de la Calculatorul gazdă B, Calculatorul gazdă A îi trimite acestuia o confirmare a numărului de secvență inițial al Calculatorului gazdă B.

În condiții normale, este configurată o conexiune, iar cele două calculatoare gazdă pot începe să schimbe date. Ce se întâmplă însă dacă expeditorul solicitării inițiale de conexiune, Calculatorul gazdă A, folosește în primul pachet o adresă IP falsificată ca adresă de sursă? Când Calculatorul gazdă B încearcă să trimită o confirmare, aceasta nu va ajunge niciodată la Calculatorul gazdă A. În final, după expirarea timpului, conexiunea este întreruptă, iar Calculatorul gazdă B eliberează memoria utilizată de conexiune.

Aceasta este metoda folosită pentru a provoca o inundare SYN. Calculatorul gazdă atacator continuă să trimită mesaje de cerere de conexiune cu o adresă IP sursă care nu poate fi găsită sau care nu există. Calculatorul gazdă care recepționează cererea continuă să aloce în memorie structuri de date și să pornească cronometre pentru încercările de conexiune până când își epuizează practic resursele și apoi începe să refuze alte încercări de conexiune. Este important ca adresa IP falsificată să fie una la care nu poate ajunge calculatorul gazdă atacat. În caz contrar, calculatorul gazdă identificat de adresa IP falsificată ar putea trimite un pachet către calculatorul gazdă atacat, având activat indicatorul de resetare care transmite calculatorului gazdă atacat să termine imediat conexiunea. Deoarece scopul inundației SYN este de a păstra resursele ocupate, acest lucru nu este de dorit.

Pentru a preveni acest tip de atac poate fi utilizat un filtru inteligent de pachete, care ține evidența pachetelor sosite care au activat bitul indicator SYN și aplică o logică simplă pentru a compara adresele IP, numerele de porturi și alte informații din antet. Când pare că se încearcă un astfel de atac, celelalte pachete care ajung la interfața externă de rețea pot fi respinse, astfel încât ele să nu ajungă la calculatorul gazdă intern care este atacat.

Redirectările ICMP și alte probleme ale protocolului ICMP

Internet Control Message Protocol (ICMP) este responsabil pentru furnizarea funcțiilor de stare și control pentru Internet Protocol. De exemplu, un server poate trimite un mesaj de tip ICMP Source Quench către un alt calculator gazdă prin care îi comunică faptul că trimite pachete la o rată prea rapidă pentru ca serverul să le poată prelucra. O altă funcție utilă implementată cu ajutorul protocolului ICMP este abilitatea de a testa cu utilitarul PING un nod de rețea pentru a determina dacă se poate ajunge la el. PING folosește pentru aceasta mesaje de tipul Echo Request (Cerere de ecou) și Echo Reply (Răspuns ecou).

Vezi și

- Pentru o listă cu tipurile de mesaje utilizate de protocolul ICMP și o descriere a funcțiilor acestora, vezi secțiunea „Protocolul ICMP (Internet Control Message Protocol)” din capitolul 2, la pagina 33.

Din nefericire, există unele tipuri de mesaje care pot fi utilizate de hackeri pentru a vă provoca probleme. Unul dintre acestea este tipul de mesaj Redirect. Acesta a fost creat pentru a permite unui ruter să comunice altui ruter că există o rută mai bună pentru o anumită destinație.

Să considerăm următorul exemplu. Ruterul B recepționează un pachet IP de la Ruterul A, care este destinat Ruterului X. Ruterul B are capacitatea de trimitere a pachetului către un alt punct în călătoria acestuia către Ruterul X, însă, consultând tabelul de rutare propriu, descoperă că există o rută mai rapidă pe care Ruterul A o poate folosi pentru a livra pachetul. În acest caz, Ruterul B poate trimite un pachet ICMP Redirect înapoi către Ruterul A pentru a-i comunica despre noua rută. Dacă Ruterul A răspunde mesajelor Redirect, actualizează propriul tabel de rutare și, de acum înainte, când dorește să trimită un pachet IP către Ruterul X, utilizează noua rută și nu mai rutează pachetul către Ruterul B.

Problema cu mesajul ICMP Redirect (și cu alte tipuri de mesaje ICMP) este că protocolul ICMP simplu nu are nici o metodă de autentificare a sursei mesajului. Acesta poate fi utilizat pentru a provoca un atac de tip interzicerea serviciului în rețeaua dumneavoastră. Nu este dificil de falsificat pachetele ICMP. Prin trimiterea de mesaje Redirect către

ruterele dumneavoastră, un intrus din exterior poate să reconfigureze tabelele de rutare din rețeaua dumneavoastră. Pe lângă acest atac de tip interdicere, mesajul Redirect poate fi utilizat pentru a provoca rutarea traficului din rețeaua dumneavoastră către unul sau mai multe calculatoare gazdă asupra cărora atacatorul are control, fiindu-i astfel mai ușor să comită și alte acțiuni reprobabile împotriva dumneavoastră.

În mod asemănător, mesajul Destination Unreachable (Destinație inaccesibilă) este utilizat pentru a comunica unui ruter că destinația unui pachet IP nu poate fi atinsă. Prin falsificarea pachetelor Destination Unreachable, un intrus din exterior poartă să îi facă pe clienții dumneavoastră să creadă că alte calculatoare gazdă importante sunt inaccesibile. Din aceste motive, este recomandată blocarea mesajelor de tip ICMP Redirect și Destination Unreachable.

În afară de faptul că este foarte util în depănarea problemelor de rețea, utilitarul PING este la fel de util atunci când încercați să adunați date despre o rețea. Una dintre funcțiile unui firewall bun este de a împiedica pe oricine din afara rețelei dumneavoastră să adune informații despre calculatoarele gazdă din rețea. Orice informație, cât de mică, pe care un hacker o poate obține îl apropie pe acesta de găsirea unei metode de pătrundere în rețeaua dumneavoastră sau de a provoca probleme în rețea. La nivelul firewall-ului, ar trebui să luați în considerare măcar blocarea mesajelor de tip ICMP Echo Request. Veți fi capabil în continuare să utilizați metoda PING pentru a testa calculatoare gazdă din afara rețelei dumneavoastră, deoarece mesajele Echo Request transmise în exterior și mesajele Echo Reply primite nu sunt blocate.

Atacuri de tip ping fatal¹

Acest atac a apărut acum câțiva ani și presupune trimiterea unui pachet ICMP supradimensionat în comparație cu un pachet Echo Request normal, care conține în mod obișnuit 64 de octeți. Trimiterea unui pachet de dimensiune mai mare decât dimensiunea maximă permisă, sau chiar mai mare de 65.536 de octeți, blochează unele sisteme de operare. Desigur, nivelul IP ar trebui să împartă un astfel de pachet în fragmente, însă atunci când ajung la calculatorul gazdă destinație, acestea sunt reasamblate și atacul reușește. Acest tip de atac nu este limitat la diferitele variante de sisteme UNIX sau Linux. Atacul de tip ping fatal s-a dovedit periculos pentru numeroase sisteme de operare.

Din fericire, toți furnizorii importanți oferă petice software care pot fi utilizate pentru a împiedica declanșarea unui astfel de atac. Dacă instalați un sistem nou folosind CD-uri sursă mai vechi de unul sau doi ani, s-ar putea să nu fiți protejat. Citiți documentația și, ca întotdeauna, verificați situsurile Web ale furnizorilor pentru a găsi actualizări și petice software pentru toate sistemele de operare pe care le utilizați.

Atacuri distribuite de tip interdicerea serviciului

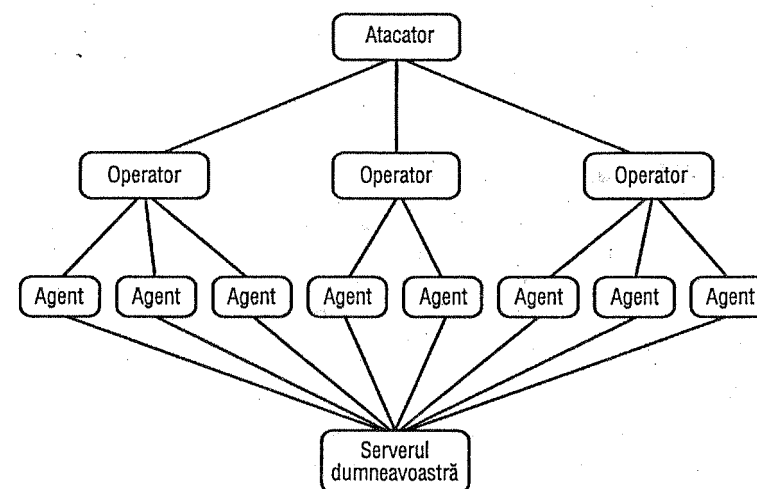
Atunci când un server este supus unui atac de tip interdicerea serviciului dinspre un singur calculator gazdă de undeva din Internet, acesta poate fi foarte nociv. Cu numai câțiva ani în urmă, au fost dezvoltate câteva seturi noi de instrumente proiectate pentru trusa

hackerului, care permit atacatorului să utilizeze mai multe calculatoare pentru a declanșa un atac zdrobitor asupra unui calculator gazdă care nu bănuiește nimic. Primul dintre aceste instrumente a fost denumit Trin00 și a fost urmat de Tribe Flood Network (TFN). A fost descoperită recent o versiune mai nouă, denumită TFN2K (de la Tribe Flood Network 2000). Cel mai nou în această gamă este un instrument care a primit numele Stacheldraht (termenul german pentru sârmă ghimpată).

Ceea ce diferențiază aceste instrumente de cele utilizate în primele forme de atacuri de tip interdicerea serviciului este natura distribuită a atacului, care este coordonat de un singur calculator gazdă administrat de atacator. În figura 3.2 puteți vedea o schemă simplă metodei de atac și să începeți să vă dați seama de ce poate fi acesta o problemă serioasă.

FIGURA 3.2

Un singur calculator atacator coordonează atacurile mai multor sisteme care se concetresc asupra unei singure ținte.



Nu este simplu de construit un astfel de atac. Inițial, atacatorul trebuie să se infiltreze în alte sisteme vulnerabile – cele care au aplicat măsuri slabe de securitate – astfel încât să poată construi un ansamblu de sisteme care să fie folosite ca operatori și agenți. Sistemele desemnate să fie agenți desfășoară atacul efectiv asupra sistemului țintă. Ele sunt controlate de sistemele desemnate de atacator să fie operatori. În partea de sus a acestei structuri de control se găsește calculatorul atacatorului.

Trin00 folosește TCP/IP pentru comunicații și este capabil să trimită un flux de pachete UDP către țintă. Instrumentele mai noi sunt mult mai sofisticate, utilizând criptarea pentru comunicații și permițând atacatorului să aleagă câteva tipuri diferite de atac. Acestea includ fluxuri UDP, SYN și ICMP sau o combinație a acestora.

Citiți mai multe despre instrumentele de atac distribuit

Pe situl Web Computer Incident Advisory Capability al organizației Lawrence Livermore National Laboratory, puteți găsi ultimele buletine de informații despre descoperirile recente, ba și o arhivă cu buletinele din ultimii câțiva ani. Buletinul CIAC-2319, „Distributed Denial of Service”, prezintă în detaliu instrumentele de atac distribuit și oferă recomandări pentru a vă apăra situl împotriva acestora. Puteți să ajungeți la situl Web CIAC folosind adresa URL:

<http://ciac.llnl.gov/>

¹ În original, Ping of Death (n.trad.)

Natura distribuită a atacului permite agenților să copleșească conexiunea de rețea a calculatorului gazdă țintă. Orice trafic legitim ce încearcă să concureze cu acest flux de pachete este fie anulat complet, fie încetinit foarte mult. Mecanismele de criptare utilizate în ultimele versiuni ale acestor instrumente și utilizarea informațiilor de adresare falsificate pot îngreuna detectarea calculatorului original utilizat de atacator pentru a declanșa atacul violent. Însă ținta acestui flux nu este singura victimă a atacului. Victime sunt și agenții care au fost infiltrați de atacator atunci când a plănuit atacul. Acești agenți nu trebuie să fie servere de mare viteză dintr-o rețea comercială. Pot fi PC-uri de la domiciliu conectate la Internet folosind DSL sau alte metode de acces de mare viteză, care rămân online cât timp calculatorul dumneavoastră este pornit.

Acest mecanism oferă atacatorului, teoretic, milioane de sisteme care pot fi incluse în forțele de atac, deoarece majoritatea utilizatorilor calculatoarelor de la domiciliu nu cunosc prea multe despre cum să își securizeze calculatoarele pentru a le proteja împotriva intruziunii inițiale.

Fragmentarea pachetelor

Nu toate legăturile de rețea folosesc aceeași dimensiune pentru cadrele de date transmise prin ele. Deoarece Internetul este o colecție foarte mare de rețele interconectate, aceasta înseamnă că este posibil ca un pachet IP, care este rutat printr-o anumită legătură, să fie mai mare decât dimensiunea permisă de legătură. Protocolul IP este capabil să împartă un pachet în mai multe pachete mai mici și să le reasambleze atunci când ajung la destinația finală.

Vezi și

➤ Pentru a revedea câmpurile de antet ale unui pachet IP, citiți secțiunea „Analiza conținutului unei datagramme IP” din capitolul 2, la pagina 43.

Există câteva câmpuri de antet dintr-o datagramă IP utilizate pentru a controla procesul de fragmentare. Câmpul Fragment Offset indică locul acestui fragment în pachetul original. Deoarece fragmentele pot să nu ajungă în ordinea în care au fost trimise și pentru că la un calculator gazdă pot ajunge fragmente amestecate din mesaje diferite, câmpul Identification este utilizat pentru a identifica fragmentele care aparțin aceluiași mesaj inițial. Câmpul Flags este utilizat pentru a arăta ce fragment reprezintă partea finală a mesajului. După ce toate fragmentele au ajuns la calculatorul gazdă, ele sunt reasamblate și trimise mai sus în stiva de protocoale.

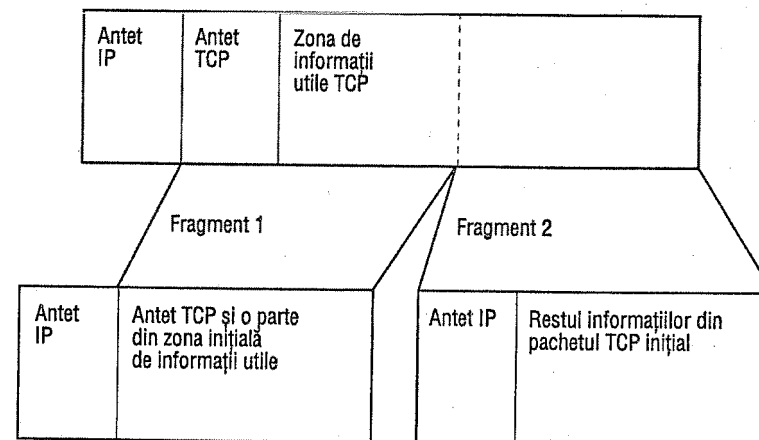
Amintiți-vă că protocolul TCP plasează propriul antet de informații în mesaje și apoi transferă rezultatul mai jos în stivă către protocolul IP, care atașează pachetului propriul antet. În acest moment, din punctul de vedere al protocolului IP, antetul TCP face parte din zona de informații utile a pachetului IP, la fel ca datele conținute de pachet. Ca urmare, atunci când protocolul IP este nevoit să fragmenteze acest pachet, antetul TCP, care se găsește la începutul zonei de informații utile, este plasat în primul fragment (vezi figura 3.3). Celelalte fragmente conțin restul pachetului TCP, însă nu conțin informații din antetul TCP.

Cât timp pachetul este reasamblat corect, nu este nici o problemă. Însă aceasta înseamnă că, atunci când fragmentele trec printr-un filtru de pachete din firewall, numai primul

pachet poate fi filtrat pe baza informațiilor de antet TCP – cum ar fi, de exemplu, numărul de port. Amintiți-vă că numărul de port pentru TCP și UDP este utilizat pentru a indica serviciul de rețea pentru care este întrebuințat pachetul. Aceasta înseamnă că, deși filtrul de pachete poate bloca primul fragment dacă violează una dintre regulile de acces stabilite de dumneavoastră, celelalte fragmente nu pot fi analizate pe baza informațiilor TCP și pot trece prin filtru.

FIGURA 3.3

Antetul TCP se găsește numai în primul fragment IP.



O șmecherie mai veche pentru trecerea unui pachet prin filtrul de pachete este pur și simplu stabilirea valorii 1 pentru câmpul destinat numărului de secvență corespunzător fragmentului din pachetul IP, astfel încât acesta să arate ca și cum ar fi un fragment dintr-un pachet mai mare. Această valoare ar trebui să fie 0 dacă ar fi primul pachet care conține informațiile de antet TCP. Deoarece ruterul presupune că fragmentul nu este primul din secvență, nu există informații de antet TCP care să fie verificate, astfel că pachetul nu este verificat potrivit regulilor pe baza cărora ruterul ar putea să blocheze anumite porturi.

Stivele TCP/IP mai vechi reasamblau uneori mai multe fragmente care au trecut prin filtru chiar dacă fragmentul cu numărul 0 nu a ajuns, atâta vreme cât fragmentele formau un pachet valid după reasamblare – aceasta însemnând că pachetul trecea verificările pentru valorile sumelor de validare. O altă metodă este de a trimite pur și simplu un pachet complet, cu numărul de secvență stabilit la valoarea 1 și bitul FIN Flag stabilit la valoarea 1, ceea ce indică faptul că este ultimul fragment.

Pentru a fi sigur că propriul calculator gazdă este protejat împotriva acestui tip de atac, revedeți documentația care îl însoțește și actualizările sau pachetele de servicii disponibile.

Virusi și cai troieni

Un firewall nu vă poate proteja de orice. Uneori, indiferent cât de bune sunt măsurile de securitate și instruirea utilizatorilor, un program rău intenționat, cum ar fi un virus sau un program de tip cal troian, pătrunde în rețeaua dumneavoastră. Virusii se pot ascunde în alte programe sau chiar în sectorul de încărcare al unui disc. Programele de tip cal troian

par să fie altceva decât sunt. Ambele pot cauza pagube însemnate dacă nu sunt detectate în timp util. Problema poate apărea atunci când un utilizator aduce software pe dischetă sau descarcă un program din Internet. De asemenea, schimburile de mesaje prin poșta electronică pot oferi o cale simplă de pătrundere în rețea.

Problema cu aceste programe distructive exista înainte ca Internetul să devină atât de popular. Acum însă, Internetul pune la dispoziția acestor tipuri de programe un mediu nou de multiplicare și distribuție. Există situri care afișează informații despre modul în care pot fi scrise aceste tipuri de programe, împreună cu mostre de cod și instrucțiuni pentru trecerea peste dispozitivele de securitate.

Unele sisteme firewall pot oferi o protecție limitată, prin faptul că pot căuta anumite indicii sau amprente digitale ale programelor virus sau de tip cal troian cunoscute. Pentru ca acest tip de software să funcționeze corect, trebuie să vă asigurați că producătorul răspunde la noile apariții în timp util și vă pune la dispoziție actualizările pentru software-ul de detecție furnizat.

Nu vă bazați numai pe capacitățile de ecranare ale firewall-ului pentru protecția față de aceste tipuri de programe. Continuați să fiți vigilenți cu privire la securitatea calculatoarelor gazdă individuale și utilizați software de scanare împotriva virușilor pe toate calculatoarele gazdă din rețea.

Poșta electronică falsificată

Falsificarea mesajelor de poșta electronică nu este un lucru dificil de realizat. Protocolul SMTP (Simple Mail Transfer Protocol) nu este foarte sigur, în special din cauza lipsei unor proceduri bune de autentificare. Dacă cineva din Internet se poate conecta la serverul dumneavoastră de poșta electronică, de obicei prin portul 25, poate să lanseze în execuție comenzile necesare pentru a trimite mesaje de poșta electronică ce par să provină de pe acel server și poate folosi orice utilizator ca sursă a poștei electronice falsificate.

Pentru cei care nu au timp să se „joace” cu protocolul SMTP, este în general ușor să configureze un client de poșta electronică astfel încât să trimită mesaje cu un nume de utilizator falsificat. După cum stau lucrurile în prezent, atunci când recepționați un mesaj obișnuit de poșta electronică, nu puteți fi sigur 100% că știți de unde provine. Datorită acestui fapt, poșta electronică falsificată poate fi foarte periculoasă în rețea. Încercați să trimiteți un mesaj de poșta electronică utilizatorilor din rețeaua dumneavoastră, cerându-le să vă trimită prin e-mail o copie a parolelor proprii. Dacă primiți răspunsuri, puteți să vă dați seama cât de periculoasă poate fi poșta electronică falsificată. Practic, poate deveni un instrument care permite unui intrus din exterior să adune informații despre rețeaua dumneavoastră sau să introducă fișiere în rețeaua dumneavoastră.

Pentru a vă ajuta să eliminați problema identificării creatorului unui mesaj de poșta electronică, puteți să utilizați *semnătura digitală* (*digital signature*). Există două avantaje ale utilizării semnăturii digitale; această metodă vă oferă:

- Autentificarea inițiatorului mesajului.
- Siguranța integrității conținutului mesajului.

Semnăturile digitale presupun utilizarea unei chei private pentru criptarea unui mesaj care poate fi citit numai utilizând cheia publică potrivită.

Vezi și

➤ Pentru mai multe informații despre modul de operare al semnăturilor digitale, vezi capitolul 9, „Tehnologii de criptare”, la pagina 166.

Intruziuni

Atunci când rețeaua locală se găsește sub controlul dumneavoastră din punct de vedere fizic, în mod normal puteți să controlați cum și când este accesată rețeaua. Chiar dacă sunt utilizate modemuri pentru a permite utilizatorilor să se conecteze la rețea, puteți să configurați modemurile pentru a fi utilizate între anumite ore și să folosiți caracteristici cum ar fi apelul invers pentru a vă apăra de potențialii hackeri. Însă o conexiune la Internet înseamnă că există milioane de potențiali hackeri asupra cărora nu aveți nici un control. Orice încredere pe care o acordați altor calculatoare gazdă din Internet reprezintă o posibilă problemă de securitate, deoarece hackerul nu trebuie decât să compromită acel sistem în care aveți încredere pentru a începe să afle mai mult despre dumneavoastră.

Furtul parolelor

Utilizarea unui cont valid de utilizator și a unei parole valide reprezintă cea mai sigură metodă de pătrundere într-o rețea. De fapt, atunci când utilizează un cont și o parolă valide, intrusul nu poate fi prins până când cineva nu suspectează acel utilizator că execută acțiuni care nu au legătură cu funcția sa. Parolele pot fi ghicite de intrus sau pot fi „sparte” prin utilizarea unui instrument de genul Crack (care descifrează parolele criptate dintr-un fișier de parole presupus a fi securizat).

O politică bună în domeniul parolelor obligă utilizatorii să aleagă parole dificil de ghicite – cu lungimea mai mare de 6 caractere, utilizând o combinație de caractere numerice și alfabetică, simboluri, litere mari și mici. Nu trebuie să stabiliți însă o politică de parole prea restrictivă. Deseori, când parolele sunt dificil de reținut, utilizatorii le scriu pur și simplu pe hârtie. Desigur, aceasta anulează întreaga rațiune de utilizare a unei parole pentru autentificare.

Instrumentele disponibile hackerilor moderni permit ca întreaga putere de prelucrare a unui calculator rapid să fie utilizată atunci când se încearcă „spargerea” unui fișier de parole criptate. Alte programe automatizează procesul de încercare repetată a conectării pentru a încerca să ghicească o parolă folosind cuvinte uzuale.

În funcție de conturile utilizatorilor, protecția bazată doar pe securitatea prin parole nu este fiabilă atunci când vă conectați într-o rețea mai mare. Pur și simplu există prea multe instrumente care fac ușor de străpuns această apărare. În locul acestei metode, poate fi utilizat un firewall ca o primă barieră în fața intrușilor din exterior, iar pentru rețelele cu cerințe ridicate de securitate, ar trebui luate în considerare tehnici mai puternice de autentificare, cu parole de unică folosință sau tokenuri fizice externe¹.

¹ token = În context are sensul de dispozitiv fizic de protecție, cum sunt, de exemplu, cartelele inteligente sau dispozitivele de recunoaștere care se pot conecta la interfețele I/O.

Vezi și

➤ Pentru mai multe informații despre tehnici mai puternice de autentificare, vezi capitolul 9, „Tehnologii de criptare“, la pagina 166.

Serviciul de clienți prietenos (social engineering)

O zonă neglijată adesea, care poate conta mult la implementarea securității, este educația utilizatorilor. Prea des, utilizatorii sunt dirijați printr-un proces de către departamentul de resurse umane, în care ei semnează niște hârtii indicând că au înțeles și că vor respecta regulile de securitate ale sitului. De fapt, mulți nici nu înțeleg tot ceea ce citesc în acele documente, și cu atât mai puțin cât de importantă poate fi securitatea. O tactică simplă de colectare a informațiilor despre o rețea este pur și simplu de a întreba pe cineva care lucrează deja în rețeaua respectivă.

Într-o secțiune anterioară, am discutat cât de ușor este de falsificat un mesaj de poștă electronică. Utilizatorii încrezători răspund de obicei cu informațiile cerute de cineva cu autoritate. De fapt, utilizatorii ar trebui să fie instruiți să nu ofere informații, cum ar fi o parolă, nici chiar unui superior. Parolele pot fi schimbate de administrator dacă este necesar accesul la un cont. Pot fi create conturi pentru utilizatorii temporari. Rareori există nevoia de a permite mai multor utilizatori să partajeze un cont sau o parolă pentru o resursă.

De asemenea, instruiți utilizatorii să verifice orice solicitare pe care o primesc prin canale nesigure, cum ar fi poșta electronică, înainte să răspundă. Instruiți utilizatorii că informațiile despre stația de lucru proprie, serverele de rețea și problemele de securitate nu trebuie să fie discutate niciodată la telefon cu persoane din afara organizației.

Intrările secrete

Atunci când un intrus din exterior a obținut chiar și un tip redus de acces în rețeaua dumneavoastră, următorul pas este de obicei să creeze un gen de punct de intrare care să îi ușureze acțiunile în viitor. Crearea unei *intrări secrete* (*backdoor*) într-o rețea poate fi la fel de simplă ca și operația de creare a unui cont nou de utilizator cu toate privilegiile pe un calculator important. Intrările secrete pot fi create utilizând programe de tip cal troian sau exploatarea eroare de programare într-o aplicație sau într-un sistem de operare. O intrare secretă într-o rețea poate fi creată chiar prin modificarea configurației firewall-ului sau a calculatoarelor gazdă care se găsesc în zona DMZ. Din nou, este un motiv pentru care securitatea calculatoarelor gazdă individuale nu ar trebui ignorată sau trecută pe al doilea plan atunci când este utilizat un firewall.

Spionarea: monitorizarea traficului de rețea

Interceptarea comunicațiilor într-o rețea LAN poate fi la fel de simplă ca și conectarea unui calculator gazdă la rețea și utilizarea unui adaptor de rețea configurat pentru modul eterogen. Vă puteți apăra de această interceptare prin monitorizarea rețelei și plasarea de elemente de control referitor la tipurile de dispozitive care pot fi atașate la rețea. În

Internet, pachetele pot fi interceptate pe orice legătură pe care călătoresc. Din acest motiv nu ar trebui folosite versiuni nesigure de utilitare de rețea, cum ar fi FTP de bază și software-ul de client Telnet. Aceste aplicații trimit numele de utilizator și parolele sub formă de text clar necriptat prin rețea.

De asemenea, Internetul nu oferă protecție pentru informațiile utile care ar putea călători în pachetele IP către sau dinspre rețeaua dumneavoastră. Singura metodă prin care puteți avea o conexiune sigură la Internet este utilizarea unei tehnologii de criptare, fie pentru fișierele individuale transmise, fie prin utilizarea unei rețele virtuale private (VPN) care creează tuneluri pentru a trece protocoalele normale de rețea printr-un flux criptat de date.

Vezi și

➤ În capitolul 10, „Rețele virtuale private (VPN) și tuneluri“, la pagina 175, puteți învăța mai multe despre tehnologiile de criptare.

Datorită faptului că un canal sigur de comunicații este atât de important și pentru că un firewall este poziționat la marginea rețelei dumneavoastră, veți găsi numeroase produse firewall ce oferă conexiuni VPN între firewall-uri.

Falsificarea IP și depersonalizarea

Într-un pachet IP, câmpul Source Address din antet este utilizat pentru a indica gazda de la care a provenit pachetul. Acesta este unul dintre câmpurile pe care le puteți configura pentru a fi analizate de un filtru de pachete, atunci când decideți ce pachete de rețea pot trece prin firewall. Există o serie de calculatoare gazdă în care aveți încredere și altele în care nu aveți încredere. Regulile de filtrare pot fi stabilite pentru a trimite mai departe sau a bloca pachetele pe baza unei adrese de gazdă sau a unei adrese de rețea.

Cum vă puteți asigura că adresa sursei este reală? Există mai multe instrumente disponibile gratuit în Internet care permit unui utilizator răuvoitor să expedieze pachete având adresa de sursă aleasă de utilizatorul respectiv. Această falsificare IP înseamnă că firewall-ul dumneavoastră poate recepționa pachete despre care crede că provin de la un calculator gazdă sau de la o rețea în care are încredere, însă în realitate sunt generate de cineva care dorește să introducă date în rețeaua dumneavoastră locală.

Gazda sigură poate fi un calculator gazdă din Internet cu care interacționați sau unul din rețeaua dumneavoastră locală. Dacă adresa IP falsificată este o adresă care pare să provină din rețeaua proprie, este ușor să configurați un filtru de pachete pentru a vă apăra, stabilind interzicerea tuturor pachetelor care ajung la interfața externă și au adresele de sursă din rețeaua dumneavoastră locală. Această operație ar trebui realizată pe toate ruterele care vă conectează la o rețea externă, deoarece legăturile de încredere dintre calculatoarele gazdă din rețeaua locală sunt configurate de obicei mai puțin strict decât cele cu gazde din Internet.

Desigur, dacă un astfel de pachet pătrunde prin filtru și gazda țintă răspunde, răspunsul este trimis către gazda identificată în câmpul pentru adresa sursei, astfel că atacatorul nu va fi capabil să vadă acel răspuns. În multe cazuri, aceasta nu contează. Problema este că prin falsificarea unei adrese IP, atacatorul poate introduce un pachet în rețeaua dumneavoastră. De exemplu, dacă atacatorul a fost capabil anterior să introducă un program de tip cal

troian în rețeaua dumneavoastră, program care „ascultă” pe un număr de port ridicat ca valoare, această metodă ar putea fi utilizată pentru a trimite în interior un pachet care ar putea instrui programul periculos să execute anumite acțiuni.

Dacă hackerul are deja anumite cunoștințe despre rețeaua dumneavoastră și este dispus să își aloce timp pentru aceasta, din falsificarea IP poate rezulta un atac și mai periculos. Acest tip de atac presupune dezactivarea unui calculator gazdă din Internet despre care se știe că este sigur pentru rețeaua dumneavoastră, și apoi depersonalizarea acelui calculator sigur. Calculatorul gazdă sigur este cel care are un tip special de acces în rețea, astfel că dacă atacatorul poate trimite în rețea un pachet care pare să provină de la o conexiune existentă pe care a configurat-o gazda sigură reală, pot rezulta pagube însemnate. Atacatorul dezactivează calculatorul gazdă sigur folosind un atac de tip interzicerea serviciului și apoi expediază către gazda dumneavoastră un pachet care pare să provină de la calculatorul gazdă sigur original.

Acest tip de atac poate fi complicat și presupune ghicirea următorului număr de secvență pentru conexiunea întreruptă. Însă operația nu este prea dificilă dacă atacatorul are cunoștințe suficiente despre protocolul TCP și despre modul în care este implementat pe gazda dumneavoastră.

Rezumat

Problemele de securitate pe care le puteți întâlni într-o rețea locală simplă sunt numeroase. Atunci când rețeaua este conectată la Internet, posibilitățile de atac sunt multiplicat. În acest capitol, ați văzut numai câteva dintre posibilele amenințări la care sunteți supus din Internet. În capitolul următor, veți analiza câteva dintre strategiile care pot fi utilizate pentru a construi un firewall și modul în care acesta vă poate ajuta să vă apărați rețeaua de aceste noi probleme de securitate.

Capitolul 4

Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor

- Proiectul precedă firewall-ul
- Strategii pentru firewall-uri
- Raportarea incidentelor și răspunsuri
- Păstrarea la zi a recomandărilor de securitate

Proiectul precedă firewall-ul

În capitolul 1, „Elemente de bază despre firewall-uri”, un firewall a fost definit ca fiind un sistem de componente desemnat să protejeze resursele din rețeaua LAN proprie împotriva persoanelor din Internet care ar vrea să vă aducă prejudicii. Componentele pe care le utilizați și modul în care le configurați nu sunt hotărâri pe care să le luați ușor. Ar trebui să vă așezați la birou și să revedeți cu atenție cerințele de securitate ale sitului dumneavoastră, după care să treceți la proiectarea unui firewall ce poate fi utilizat pentru a impune respectarea cu strictețe a acestei politici de securitate.

Cu toate că ați putea fi tentat să ascultați de echipa de vânzări a unui furnizor și să cumpărați pur și simplu ultimul tip și cel mai bun (după cum spun ei) de firewall, nu este cea mai înțeleaptă acțiune. S-ar putea să fie simplu să vă bazați pe documentația pusă la dispoziție de echipele de vânzări și pe promisiunile făcute de un furnizor cu care faceți des afaceri. Relațiile de acest tip pe termen lung presupun de obicei că furnizorul nu încearcă să vă vândă ceva doar pentru a vinde. Însă o dată cu noile companii de software care apar peste tot, s-ar putea să vă dați seama că ați achiziționat o soluție de firewall de la o companie care nu are resurse corespunzătoare pentru asistență tehnică. Dacă furnizorul dumneavoastră nu poate să vă sprijine, s-ar putea să vă dați seama că sunteți total nepregătit atunci când are loc un eveniment important care afectează securitatea rețelei.

Pe baza politicii de securitate a companiei, puteți să creați o politică de securitate pentru firewall. Chiar dacă întreaga politică de securitate a companiei s-ar putea să fie formată din mai multe documente și să acopere o gamă largă de subiecte, politica de securitate pentru firewall vă oferă detalii despre modul de implementare a firewall-ului astfel încât să poată fi utilizat pentru a impune respectarea cerințelor de securitate atunci când acestea au legătură cu conexiunile realizate prin firewall.

Politica de securitate a companiei dumneavoastră

Ce este o politică de securitate? Descrisă simplu, este specificarea a ceea ce poate fi făcut și a ceea ce nu poate fi făcut pe un calculator sau într-o rețea. Deși aceasta ar putea suna prea simplu, o politică bună de securitate cuprinde multe subiecte diferite și descrie în detaliu acțiunile permise utilizatorilor, ca și pedepsele impuse în cazul în care se constată un comportament necorespunzător. Un contraargument la o politică de securitate detaliată este acela că utilizatorul s-ar putea să nu înțeleagă tot sau chiar să nu o citească dacă este prea lungă. Totuși, este preferabil să lăsați utilizatorii să afle de la început ce este permis și ce nu, decât să ajungeți mai târziu să vă certați asupra detaliilor. Dacă nu credeți ce vă spun, consultați compartimentul juridic (în cazul în care aveți unul)!

O politică de securitate ar trebui formulată în unul sau mai multe documente scrise. Înainte de a permite unui angajat să utilizeze o resursă de calcul, ar trebui să îi cereți să revadă documentația privitoare la securitate și să confirme faptul că a citit-o. În majoritatea organizațiilor comerciale mari, această funcție este îndeplinită de departamentul de resurse umane și constă în general din câteva documente, cum ar fi politica de conectare la rețea și o specificație de utilizare acceptabilă care trebuie semnate de angajat. În plus, ați putea să realizați un document care descrie acțiunile ce trebuie efectuate în cazul în care este descoperită o problemă de securitate.

Politica de conectare la rețea

O politică de conectare la rețea ar trebui să descrie tipurile de dispozitive pentru care permiteți conectarea la rețea. De exemplu, chiar dacă în mod sigur vreți să permiteți conectarea la rețea a unor servere de rețea și a unor stații de lucru pentru utilizatori, s-ar putea să nu doriți conectarea unui server de terminale echipat cu un banc de modemi. În mod similar, politica de conectare la rețea ar trebui să detalieze modul în care trebuie configurate sistemele permise în rețea. Această politică ar putea include și elemente cum ar fi:

- Modul în care trebuie instalat sistemul de operare, ce funcții trebuie utilizate și detalii despre modul în care trebuie configurate sistemul de operare și aplicațiile.
- Unde pot fi instalate în cadrul rețelei (subrețeaua fizică) anumite tipuri de sisteme și modul în care sunt tratate problemele de adresare în rețea.
- Software-ul de protecție împotriva virusilor trebuie instalat și actualizat regulat, după cum este nevoie.
- Drepturile utilizatorilor și protecțiile resurselor puse la dispoziție de sistemul de operare trebuie configurate într-un mod specificat.
- Procedurile care trebuie parcurse pentru a obține un cont nou de utilizator și, ca un subiect similar, procedurile care trebuie parcurse la dezactivarea unui cont de utilizator.
- Instalarea de componente hardware sau software suplimentare, neaprobată de administratorul de rețea (sau de altă autoritate responsabilă), este strict interzisă.

Desigur, aceasta nu este o listă completă. Ar trebui să vă bazați conținutul politicii specifice de conectare la rețea pe cerințele sitului dumneavoastră. De exemplu, dacă aveți utilizatori cu calculatoare laptop, le veți permite să se conecteze la rețea sau îi obligați să schimbe date cu calculatoarele desktop prin alte metode, cum ar fi o dischetă sau un alt

dispozitiv de stocare amovibil? Dacă permiteți conectarea calculatoarelor laptop la rețea, este configurat fiecare laptop cu o adresă specifică de rețea sau utilizați protocolul DHCP pentru configurarea rețelei? Mai mult, îi veți permite utilizatorului să conecteze laptopul și la alte rețele, cum ar fi rețeaua unui client, atunci când se află în deplasare?

De asemenea, politica de conectare la rețea ar trebui să ia în considerare funcțiile pentru care sunt utilizate anumite calculatoare. Chiar dacă ați putea permite unui departament să configureze un server Web sau un server FTP, politica ar trebui să specifice clar unde trebuie conectat în rețea acest tip de server. De exemplu, într-o secțiune viitoare din acest capitol veți învăța cum să creați o *zonă demilitarizată* care poate fi utilizată pentru a permite accesarea acestor tipuri de servere de către clienții dumneavoastră prin Internet, fără a permite ca acest tip de trafic de rețea să circule prin întreaga rețea LAN.

Ce ar trebui să includă o bună politică de securitate?

Înainte să începeți să scrieți o politică de securitate sau să o actualizați pe cea curentă, este bine să citiți un document foarte bun, RFC 1244, denumit „Ghidul securității sitului”. Acest document RFC conține o listă de resurse comune pentru numeroase rețele și descrie câteva probleme potențiale de securitate.

O specificație de utilizare acceptabilă

Un calculator desktop este, probabil, cel mai folosit instrument de afaceri în prezent. Aceasta înseamnă că, pe lângă funcțiile sale importante pentru afaceri, cum ar fi aplicațiile de prelucrare de texte și de baze de date, calculatorul poate să fie utilizat și pentru rularea de jocuri și de alte programe care nu au nimic de-a face cu sarcinile de lucru ale utilizatorului respectiv. Există și alte aparate, cum ar fi fotocopiatorul și telefonul, care sunt deseori întrebuințate în exces, însă probabil nu la nivelul la care este utilizat calculatorul desktop. Atunci când utilizați o conexiune la Internet, potențialul pentru întrebuințare abuzivă crește enorm!

Probabil că nu vă pasă dacă un colaborator folosește ocazional telefonul pentru a verifica o programare la doctor sau folosește fotocopiatorul pentru a face o copie a unei declarații de venituri. Astfel de acțiuni neînsemnate nu costă prea mult organizația. Mai mult, în anumite privințe, această „utilizare abuzivă” trecută cu vederea poate fi considerată un avantaj pentru angajat. Atunci când analizați însă tipurile de activități pentru care poate fi utilizat calculatorul, costurile implicate nu mai pot fi considerate neînsemnate. Nu trebuie decât ca un utilizator să încarce pe calculator un program de pe o dischetă pentru a lansa în execuție un virus care se împrăștie în toată rețeaua. Pentru ca organizația dumneavoastră să fie dată în judecată, nu este nevoie decât ca un singur angajat să scrie un mesaj de poștă electronică defăimător către alt angajat sau, foarte posibil, către unul dintre clienții importanți ai companiei.

Datorită potențialului ridicat al utilizării incorecte și al abuzurilor, este important să specificați clar tipurile de activități pentru care poate fi utilizat calculatorul și ce tipuri de acțiuni sunt inacceptabile. O specificație de utilizare acceptabilă este o metodă bună pentru a realiza acest obiectiv.

Iată câteva dintre lucrurile pe care le puteți lua în calcul pentru a fi incluse într-o specificație de utilizare acceptabilă:

¹ În original, „Site Security Handbook” (n.trad.)

- Nu este permisă instalarea pe calculator a nici unei aplicații care nu este aprobată sau furnizată de companie. Între acestea sunt incluse copii „ilegale” ale unor programe aduse de pe un calculator de la domiciliu, ca și programele shareware care pot fi descărcate cu ușurință din Internet.
- Nici o aplicație furnizată de companie nu poate fi copiată pentru a fi utilizată în altă parte, cum ar fi pe calculatorul de la domiciliu al utilizatorului.
- Atunci când un utilizator pleacă de lângă stația de lucru, aceasta nu trebuie lăsată conectată în rețea cu un cont de utilizator. Sau, pentru protejarea stației de lucru atunci când este lăsată nesupravegheată, trebuie utilizat un program de protecție a ecranului care folosește o parolă.
- Orice activitate dubioasă trebuie raportată autorității corespunzătoare.
- Calculatorul și aplicațiile pe care le conține nu pot fi utilizate sub nici o formă pentru a hărțui sau a amenința o altă persoană.
- Poșta electronică nu poate fi utilizată în scopuri personale.
- Încercarea de a accesa date care nu sunt de interes pentru postul utilizatorului, ceea ce se numește uneori *sondarea rețelei*, nu este permisă.

Dacă oricare dintre aceste restricții vă sună prea sever, gândiți-vă la posibilitățile care pot rezulta din nerespectarea lor. De exemplu, în Internet sunt mii și mii de programe shareware și freeware disponibile pentru descărcare. Dacă, de exemplu, permiteți unui angajat să descarce un fișier care conține imagini grafice care pot fi folosite în documentele companiei, aceasta s-ar putea să nu pară un lucru prea periculos. Vă gândiți însă că fișierul descărcat conține un virus de calculator? Vă gândiți că fișierul freeware este în realitate o copie a unui material protejat prin legea drepturilor de autor? Au toți utilizatorii dumneavoastră capacitatea de a lua decizii cu privire la ce fișiere sunt periculoase și ce fișiere nu sunt?

Nici în acest caz lista precedentă nu este o listă completă, cu toate lucrurile pe care ar trebui să le introduceți într-o specificație de utilizare acceptabilă. Evaluați mediul în care se desfășoară activitățile organizației dumneavoastră pentru a ajunge la o astfel de listă. Discutați regulile de utilizare cu conducătorii din toate departamentele astfel încât să puteți înțelege ceea ce așteaptă ei de la rețea și încercați să ajungeți la o politică ce permite utilizatorilor să își îndeplinească obligațiile fără a compromite rețeaua și fără să implice compania în probleme juridice.

Politici severe de securitate

Înainte de toate acestea, ar trebui reținut faptul că o politică de securitate trebuie să fie rezonabilă și nu prea severă. Cu toate că trebuie să includeți interdicții pentru acțiunile care pot deveni probleme de securitate, doriți să vă asigurați că lăsați suficientă libertate pentru ca utilizatorii să-și îndeplinească sarcinile. Confruntat cu o politică absolută și cu un administrator de securitate care nici nu îl ascultă, nici nu îl înțelege, un utilizator poate găsi alte mijloace pentru a-și îndeplini sarcinile, mijloace care pot provoca mai multe probleme decât intenția inițială. Dacă utilizatorii solicită noi aplicații software sau permisiunea de a folosi un produs shareware, un bun administrator evaluează corect cererile. Dacă aplicația este utilă, poate fi testată într-un laborator înainte de a fi instalată în rețea.

Angajați, colaboratori și furnizori externi de servicii

O bună politică de securitate parcurge un drum lung până ajunge să vă protejeze resursele de rețea de utilizări eronate și abuzuri. Probabil că vă veți da seama că este dificil să anticipați toate situațiile care pot apărea. Din acest motiv, este recomandat să discutați cu

utilizatorul nu doar elementele specifice ale politicii de securitate, ci și să îi explicați motivele care au condus la formularea acestei politici.

Interzicerea sondării rețelei este un bun exemplu de subiect pe care îl puteți discuta. Numeroși utilizatori ar putea să lucreze având în minte ideea că „dacă accesul nu este blocat, nu greșesc cu nimic dacă mă uit și eu”. Ar trebui să îi faceți să înțeleagă că, deși este posibil să utilizați drepturi și permisiuni pentru a împiedica accesarea datelor de către cei care nu ar trebui să o facă, există întotdeauna posibilitatea de a uita ceva. Faceți-i pe utilizatori să înțeleagă faptul că dacă ceva nu are legătură cu funcția lor, nu ar trebui să se uite. Acest lucru este valabil și pentru copiii hard. La fel cum nu aveți nici o justificare să vă uitați peste umărul cuiva și să îi citiți mesajele de poșta electronică, ar trebui să nu citiți rapoartele care ies de la imprimantă în timp ce așteptați terminarea lucrării dumneavoastră de tipărire.

Pentru a exprima foarte concis cele explicate anterior, asigurați-vă că utilizatorii înțeleg că într-un mediu de lucru, este de așteptat să aibă un comportament etic!

Cu toate că ar putea părea evident faptul că veți avea un document scris referitor la politica de securitate, pe care un angajat va trebui să îl citească și să îl accepte înainte să îi fie permisă folosirea rețelei, nu lăsați o breșă în procedurile de securitate, uitându-i pe alții care ar putea avea nevoie să utilizeze rețeaua.

Colaboratorii externi reprezintă o metodă foarte răspândită de rezolvare a proiectelor pe termen scurt și, în anumite cazuri, costurile justifică finanțarea pozițiilor pe termen lung cu utilizatori care nu sunt angajați ai companiei. Acești utilizatori nu ar trebui să fie trecuți cu vederea atunci când se creează o politică de securitate. De asemenea, nu ar trebui uitați nici furnizorii, care asigură asistență atunci când aveți probleme cu software-ul sau hardware-ul. În cazul în care creați un cont de utilizator care va fi folosit de o astfel de persoană, s-ar putea să fie nevoie ca furnizorul să cunoască și să accepte politica dumneavoastră de securitate.

Pirateria software

Realizarea de copii ilegale de produse software este o problemă larg răspândită. Mulți utilizatori nici nu se gândesc la faptul că în realitate fac o infracțiune atunci când realizează o copie a unui program și o rulează pe propriul calculator de la domiciliu. Este important să luați măsuri pentru ca toți utilizatorii dumneavoastră să înțeleagă consecințele pirateriei software. Dacă aveți nevoie de ajutor pentru a vă decide cum să impuneți un program bun anti-piraterie în compania dumneavoastră, puteți să vizitați situl Web al organizației Software & Information Industry Association, la adresa www.s.i.i.a.com. Această organizație este rezultatul unei fuziuni care a avut loc la 1 ianuarie 1999 între Software Publishers Association (SPA) și Information Industry Association (IIA).

Politica pentru firewall

Deseori politica de securitate este confundată cu *politica pentru firewall (firewall policy)*. După ce ați proiectat politica de securitate și ați decis ce servicii și protocoale veți permite să treacă prin firewall și în ce direcție, trebuie să hotărâți cum să implementați această politică în firewall. Prin proiect, un firewall folosește reguli pentru a decide ce pachete (în cazul unui filtru de pachete) sau servicii (în cazul unui serviciu intermediar sau al unei porți de aplicație) pot trece. Politica poate avea una dintre următoarele variante:

- Permite orice acces, mai puțin în cazul în care a fost interzis explicit de reguli.
- Interzice orice acces, mai puțin în cazul în care a fost permis explicit de reguli.

Chiar dacă aceste două politici vi se par destul de simple și v-ați putea gândi că nu este o diferență prea mare între ele, nu este așa. Dacă folosiți prima politică, trebuie să creați pe firewall reguli care să poată lua în considerare fiecare împrejurare în care ar trebui utilizată o interdicție. În afară de faptul că pot rezulta o mulțime de reguli prin proiectare, această politică vă lasă fără protecție de fiecare dată când apare un protocol sau un serviciu nou, care nu este acoperit de regulile dumneavoastră.

A doua politică este mai simplă și mai sigură. Dacă interziceți explicit tot traficul de rețea care trece prin firewall și oferiți numai regulile necesare pentru a acorda acces prin firewall anumitor instanțe de care aveți nevoie, aveți un control mult mai sigur asupra firewall-ului. În acest tip de situație, potențialul intrus trebuie să găsească mijloace pentru a specula condițiile limitate pe care le-ați stabilit pentru acordarea accesului.

În continuare, specificați căror servicii le veți permite trecerea prin firewall și în ce direcție. Puteți decide acest lucru analizând în ansamblu politica de securitate. De exemplu, dacă nu permiteți descărcarea fișierelor din Internet, trebuie să aveți un articol în politica pentru firewall prin care să interziceți folosirea protocolului FTP către interior. Dacă vă îngrijorează utilizatorii care folosesc protocolul FTP pentru a trimite date confidențiale sau fișiere de program către calculatoare din afara companiei, aveți nevoie de un articol care să interzică protocolul FTP către exterior. De asemenea, ați putea restricționa și alte servicii, cum ar fi Telnet sau HTTP.

Este important să lucrați împreună cu utilizatorii sau măcar cu managerii lor pentru a determina ce servicii de rețea sunt cu adevărat necesare. Într-adevăr, chiar dacă v-ați putea decide să interziceți în mod special serviciile FTP către interior și către exterior, cum veți mai obține noile versiuni de software, actualizările sau peticele? Ați putea specifica interzicerea oricărui acces FTP și apoi să asigurați o excepție pentru un calculator gazdă foarte bine securizat, care permite doar conectarea anumitor utilizatori. O altă soluție este să folosiți un calculator care nu este conectat la rețeaua LAN proprie, dar care are acces la Internet pe linie telefonică și poate fi utilizat pentru o astfel de funcție.

Între elementele pe care decideți să le implementați utilizând firewall-ul s-ar putea număra și următoarele:

- Poșta electronică este permisă pentru clienți către și din Internet, însă trebuie să treacă printr-un server SMTP securizat.
- Nu este permis nici un serviciu care presupune o conexiune directă de rețea între un client intern și un serviciu extern. Orice serviciu permis trebuie să utilizeze un server intermediar.
- Accesul Telnet către exterior este permis pentru utilizatorii din departamentul de cercetare și dezvoltare, însă este interzis tuturor celorlalți utilizatori. Nu este permis nici un acces Telnet către interior. Utilizatorii care sunt autorizați să se conecteze la rețea de la o sursă externă folosesc un modem instalat pe un server securizat, plasat într-o subrețea ecranată.
- Este interzis accesul FTP către interior și către exterior.
- Serverele DNS dintr-o subrețea securizată permit rezolvarea numelor calculatoarelor firewall și intermediar de aplicație, însă nu li se permite să rezolve numele pentru clienții din rețeaua LAN internă.

Aceasta este o listă scurtă. Este ușor să creați o listă scurtă dacă respectați principiul că totul este interzis, cu excepția lucrurilor permise explicit.

Pe lângă specificarea tipurilor de servicii care vor fi permise și modul în care vor fi implementate (adică server intermediar sau filtru de pachete, pentru toți utilizatorii sau pentru gazdele selectate), ar trebui să includeți în politica de firewall și elementele în care specificați cât de des sunt revăzute fișierele jurnal, cum sunt configurate alarmele și așa mai departe.

În final, vă recomand să fiți flexibil atunci când analizați solicitările utilizatorilor și faceți excepții, însă nu mergeți prea departe, creând atât de multe excepții încât firewall-ul să devină inutil pentru orice scop practic!

Strategii pentru firewall-uri

După ce ați determinat care ar trebui să fie cerințele de securitate pentru situl dumneavoastră și ați formulat o politică bine scrisă, puteți să începeți procesul de proiectare a firewall-ului. Componentele pe care le utilizați depind de tipurile de servicii pe care doriți să le faceți disponibile pentru utilizatorii din rețeaua LAN proprie. Serviciile pe care le alegeți depind de modul în care sunt legate serviciile de acțiunile permise de politica dumneavoastră de securitate.

Cele două componente de bază pe care le puteți utiliza pentru a construi un firewall sunt următoarele:

- Un filtru de pachete
- Un server intermediar de aplicație

Ați putea folosi doar una dintre aceste variante sau pe ambele. Componentele pot fi implementate în diferite moduri pentru a oferi diferite niveluri de securitate. Modul în care configurați componentele firewall-ului poate fi considerat ca fiind *arhitectura* firewall-ului. Arhitecturile pe care le veți lua în considerare sunt următoarele:

- Un ruter sau calculator gazdă cu funcția de filtrare a pachetelor
- O poartă cu două plăci de rețea
- O gazdă ecranată
- O subrețea ecranată

Utilizarea unui filtru de pachete

În prezent, firewall-urile pot fi formate din unul sau mai multe rutere sau calculatoare gazdă pe care rulează software de firewall ce folosește diferite metode pentru a acorda sau a interzice accesul la și din rețeaua LAN locală. Însă primul tip de firewall utilizat pe scară largă a fost un simplu *ruter cu ecranare (screening router)*, care este numit în mod uzual *filtru de pachete (packet filter)*.

Vezi și

- Pentru o discuție mai detaliată privitoare la utilizarea filtrării pachetelor în firewall-uri, vezi capitolul 5, „Filtrarea pachetelor”.

Un *ruter (router)* este un dispozitiv de rețea configurat cu mai multe interfețe și atașat la două sau mai multe rețele. Atunci când un calculator din rețea trebuie să trimită un pachet

la un calculator situat într-o altă rețea, trimite pachetul la adresa ruterului și lasă ruterul să determine cea mai bună metodă pentru livrarea informațiilor către destinația finală. Ruterul ia aceste decizii în funcție de informațiile de adresare pe care le găsește în antetul pachetului.

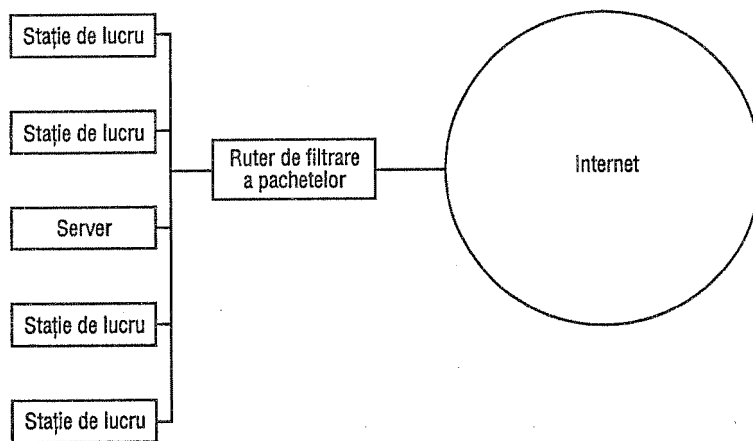
Dacă ruterul determină faptul că pachetul este destinat unei gazde care se găsește într-o subrețea conectată direct cu una dintre propriile interfețe de rețea, pachetul este retransmis rapid la acea interfață, astfel încât își poate termina călătoria. Dacă ruterul determină că pachetul nu este destinat nici uneia dintre rețelele care îi sunt atașate direct, trimite pachetul către alt ruter (următorul „salt” din călătorie) care ar putea să știe cum să trimită pachetul către destinația finală. Desigur, dacă ruterul nu cunoaște nici un alt dispozitiv care ar putea livra pachetul, poate să îl respingă pur și simplu și să returneze un mesaj ICMP către sursă, pentru a-i comunica ceva de genul „nu puteți ajunge acolo de aici”.

Un *ruter cu ecranare* (*screening router*) este un ruter configurat cu un set de reguli care specifică ce tip de trafic de rețea este permis, într-un sens sau în celălalt, prin interfețele de rețea atașate ruterului. Cu alte cuvinte, după ce ruterul a decis că poate livra pachetul (fie către următorul dispozitiv, fie direct către destinația finală), consultă un set de reguli care îi spun dacă *ar trebui* să ruteze pachetul.

De exemplu, să presupunem că ruterul recepționează un pachet de la o gazdă de undeva din Internet care face o cerere pentru a stabili o sesiune Telnet cu o gazdă din rețeaua LAN internă. Desigur, ruterul decide de la început că știe cum să ruteze pachetul – îl retransmite pe aceeași interfață la care este atașată gazda destinație, după ce inițial a plasat adresa MAC a gazdei destinație în pachet, astfel încât să fie recunoscut de gazdă. Însă, deoarece este un ruter de ecranare, în continuare trebuie să fie analizate regulile. Regulile spun că toate cererile de sesiuni Telnet sosite din exterior trebuie să fie refuzate. Astfel, așa cum puteți vedea și din figura 4.1, gazdele din rețeaua LAN internă sunt protejate de posibila compromitere de către un intrus care folosește utilitarul Telnet ca metodă de pătrundere.

FIGURA 4.1

Un filtru de pachete decide ce pachete pot călători între rețeaua LAN proprie și Internet.



Această metodă fundamentală de filtrare este numită *filtrarea pachetelor independent de stare* (*stateless packet filtering*), deoarece fiecare pachet este analizat după propria valoare – după datele pe care le conține în antet. O metodă mai nouă de filtrare a pachetelor, numită

filtrarea pachetelor în funcție de stare (*stateful packet filtering*) sau *inspectare în funcție de stare* (*stateful inspection*), duce procesul cu un pas mai departe, păstrând în memorie informații care înregistrează starea sesiunilor curente. Atunci când este recepționat un pachet care pretinde că este un răspuns la un pachet care a fost trimis din rețeaua dumneavoastră locală către exterior, filtrul de pachete dependent de stare verifică în tabelele sale pentru a vedea dacă pachetul este într-adevăr un răspuns la o cerere trimisă anterior în exterior. Astfel, atunci când folosiți într-un filtru de pachete tehnici de inspectare dependente de stare, este mult mai dificil pentru un potențial intrus să introducă în rețea un pachet care conține informații de adresare falsificate.

Chiar dacă în discuția de până acum a fost folosit ca filtru de pachete un ruter, puteți găsi capacități de filtrare a pachetelor în majoritatea produselor firewall din comerț. În multe cazuri, software-ul de filtrare a pachetelor care rulează pe un calculator gazdă este de preferat unui ruter, deoarece este mai ușor de folosit și are funcții de înregistrare a evenimentelor. Ruterul pot fi dificil de configurat, în special când cerințele dumneavoastră impun un număr mare de reguli. Modificarea unui set mare de reguli poate necesita mult timp, deoarece trebuie să verificați fiecare regulă pentru a fi sigur că această modificare nu blochează sau permite ceea ce încercați să obțineți cu o regulă nouă! De asemenea, ruterul sunt cunoscute pentru faptul că nu posedă capacități de înregistrare a evenimentelor. Un produs firewall bun oferă funcții detaliate de înregistrare a evenimentelor și de avertizare și, probabil, software care poate fi utilizat pentru a analiza fișierele jurnal.

Ce informații poate să utilizeze un filtru de pachete?

Un filtru de pachete operează pe baza informațiilor pe care le găsește în antetul pachetului de rețea, și există diferite produse capabile să efectueze filtrări pe baza următoarelor informații:

- Adresa IP sursă și adresa de destinație
- Protocolul (cum ar fi TCP, UDP sau ICMP)
- Porturile sursă și destinație TCP sau UDP
- Tipul mesajului, dacă este ICMP

În plus, o altă informație importantă de care dispune filtrul de pachete, care nu are legătură cu informațiile din antetul pachetului, este interfața la care ajunge pachetul. Aceasta este o informație foarte importantă! De exemplu, dacă un filtru recepționează un pachet pe interfața care realizează conectarea cu rețeaua externă și descoperă că pachetul are o adresă sursă care pare să provină din rețeaua dumneavoastră LAN, este clar că va refuza acest pachet falsificat, deoarece nu ar fi posibil ca pachetul să ajungă la interfața externă folosind această adresă.

Utilizarea unei porți intermediare de aplicații

Un filtru de pachete nu poate decât să ia decizii bazate pe informațiile care se găsesc în antetul pachetului. Din nefericire, aceste informații sunt, în cea mai mare parte, date de adresare și alte informații referitoare la pachet de care are nevoie protocolul pentru a deplasa pachetul printr-un labirint de rețele în vederea livrării. Datele din antetul pachetului nu comunică filtrului de pachete detalii specifice care pot fi folosite pentru a decide în cunoștință de cauză dacă pachetului ar trebui să i se permită să traverseze firewall-ul. De exemplu, un ruter poate determina că scopul pachetului este un anumit protocol, cum ar fi

FTP. Însă ruterul nu poate spune dacă cererea de sesiune FTP este o cerere de tip „put“ (scriere) sau „get“ (aducere). Chiar dacă nu ați reține cererile „get“ destinate unei anumite gazde, în general nu vreți să fie permisă trecerea cererilor „put“ pentru această gazdă.

Vezi și

- Pentru mai multe informații despre porți de aplicație și servere intermediare, vezi capitolul 7, „Porți de aplicații și servere intermediar“.

O *poartă de aplicație* (*application gateway*) sau un *server intermediar de aplicație* (*application proxy*) este un program software care rulează pe firewall pentru a intercepta traficul pentru un anumit tip de aplicație. Software-ul intermediar interceptează cererile utilizatorilor din rețeaua LAN proprie, de exemplu, și apoi realizează pentru utilizatorul dumneavoastră o conexiune cu serverul care se găsește în afara rețelei locale. Utilizatorul intern nu realizează niciodată o conexiune directă cu serviciul din exterior. Programul intermediar de aplicație acționează ca un intermediar și discută cu clientul și cu serverul, distribuind informații despre aplicație între aceștia. Avantajul acestei soluții este acela că intermediarul de aplicație poate fi programat să permită sau să interzică traficul pe baza informațiilor conținute în secțiunea cu date utile a pachetului, și nu doar pe baza informațiilor din antet.

Un dezavantaj al programelor intermediare este însă acela că sunt specifice aplicațiilor. Pentru fiecare serviciu sau aplicație pentru care doriți să aveți suport pe firewall trebuie dezvoltată câte o aplicație intermediară separată. Un alt dezavantaj este acela că software-ul client trebuie să fie capabil să lucreze cu aplicația server intermediar. Majoritatea pachetelor software mai noi sunt proiectate cu această caracteristică, astfel că nu este nici o problemă. De exemplu, și browserul Navigator produs de Netscape, și browserul Internet Explorer produs de Microsoft vă permit să specificați servere intermediare (dacă sunt utilizate în rețea astfel de produse).

Vezi și

- Pentru mai multe informații despre traducerea adreselor de rețea, vezi secțiunea „Traducere de adrese de rețea (NAT)“ din capitolul 7, „Porți de aplicații și servere intermediar“.

Pot fi făcute să lucreze chiar și programele mai vechi, care nu înțeleg serverele intermediare. De exemplu, folosind Telnet, un utilizator poate să se conecteze inițial la un server intermediar și să fie validat de acest server înainte să i se permită să creeze o sesiune Telnet cu o gazdă externă. Această metodă din două operații nu este la fel de bună ca metoda transparentă pusă la dispoziție de aplicațiile client care au fost programate să lucreze cu servere intermediare.

O altă zonă care trebuie explorată dacă doriți să adaptați aplicațiile astfel încât să lucreze cu servere intermediare este folosirea programului Trusted Information Systems Internet Firewall Toolkit (FWTK) sau a unui pachet cum ar fi SOCKS. SOCKS oferă o bibliotecă de programare care poate fi utilizată pentru crearea sau modificarea clienților pentru a interacționa cu o aplicație server intermediar SOCKS. Programul TIS Firewall Toolkit poate fi folosit pentru a crea servicii intermediare pentru numeroase servicii uzuale, cum ar fi Telnet, FTP și HTTP.

Vezi și

- Pentru mai multe informații despre SOCKS, vezi capitolul 15, „SOCKS“.
- Pentru mai multe informații despre TIS Firewall Toolkit, vezi capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)“.

Ce este traducerea adreselor de rețea?

O formă de server intermediar foarte răspândită în prezent este translatorul de adrese de rețea (Network Address Translator, sau NAT). Acest tip de server vă ajută să îmbunătățiți securitatea rețelei ascunzând informațiile despre adresele reale utilizate în rețeaua LAN internă. Translatorul realizează aceasta utilizând propria adresă IP validă atunci când face cereri intermediare către servicii din exterior pentru clienții din rețeaua LAN internă. Un alt avantaj care face ca translatorul NAT să fie foarte răspândit este acela că, datorită faptului că numai serverul intermediar trebuie să folosească o adresă validă în Internet, sunteți liber să utilizați aproape orice domeniu de adrese IP pentru clienții rețelei LAN interne. Deoarece spațiul de adrese din Internet se diminuează foarte rapid, această tehnică poate fi utilizată pentru a extinde rețeaua LAN internă fără a trebui să obțineți de la început un domeniu mare de adrese de la furnizorul de servicii Internet.

Combinații

După cum puteți vedea, atât filtrele de pachete cât și serverele intermediare pot fi folosite pentru a crea un firewall, și fiecare metodă are propriile avantaje și dezavantaje.

De asemenea, probabil ați ghicit că următorul pas este combinarea celor două variante pentru a obține o soluție mai sigură de firewall. Atunci când utilizați atât un filtru de pachete, cât și unul sau mai multe produse intermediare de aplicație, începeți să înțelegeți de ce un firewall este mai mult un sistem decât o singură entitate.

Există mai multe metode prin care puteți combina aceste două tehnologii. Însă, indiferent de modul în care configurați filtrul de pachete sau de modul în care lucrați la proiectarea unui intermediar de aplicație, întotdeauna este posibil să aveți nevoie de o altă soluție. Atunci când proiectați firewall-ul, ar trebui să analizați avantajele și dezavantajele fiecărei strategii pentru a decide care dintre ele se aplică mai bine cazului dumneavoastră. Din nou, revedeți politica de securitate și alegeți o arhitectură de firewall prin care să puteți oferi cea mai bună aplicare a acelei politici.

Atunci când revedeți aceste strategii, veți întâlni termeni cum ar fi *gazdă bastion* (*bastion host*) și *DMZ*. Acești termeni descriu componente importante ale firewall-ului care, atunci când sunt folosite corespunzător, pot să vină în întâmpinarea unui firewall securizat. Acești termeni sunt analizați în detaliu în alte secțiuni din acest capitol.

De ce ar trebui să folosiți atât un filtru de pachete, cât și un software intermediar?

După cum spune un vechi proverb, nu puneți toate ouăle în același coș. Ultimul lucru pe care îl doriți într-un mediu securizat este să aveți un singur punct în rețea care, atunci când cedează, deschide accesul către toată rețeaua. Un filtru de pachete poate să asigure un gen de protecție, iar produsele intermediare de aplicație merg și mai departe pentru a împiedica traficul nedorit să circule între rețeaua LAN internă și rețeaua externă. Dacă serverul intermediar de aplicație se blochează (se poate întâmpla), aveți la dispoziție în continuare filtrul de pachete ca o primă linie de apărare până când reparați serverul intermediar.

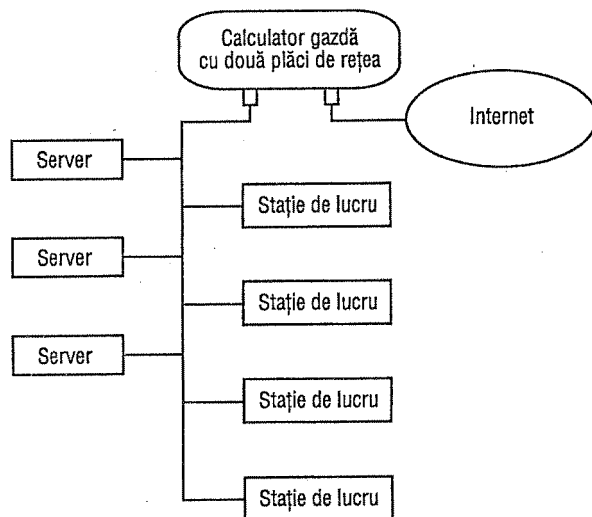
Utilizarea unui calculator gazdă cu două plăci de rețea

Un ruter care conectează rețeaua la Internet trebuie să aibă cel puțin două interfețe de rețea. Una este folosită pentru conectarea la rețeaua LAN proprie, iar cealaltă realizează conexiunea cu lumea exterioară. Fiecare interfață de rețea are o adresă IP unică. Pe baza regulilor pe care le stabiliți, ruterul ia decizii referitoare la pachetele care trebuie retransmise de la o interfață la alta.

O gazdă cu două plăci de rețea (*dual-homed host*) funcționează într-un mod asemănător. Un calculator este configurat cu două interfețe de rețea și, la fel ca ruterul, un adaptor este conectat la rețeaua LAN internă, iar celălalt realizează conexiunea la Internet (vezi figura 4.2). Însă, spre deosebire de un ruter, multe sisteme de operare recunosc faptul că au fost instalate două adaptoare și retransmit automat pachetele de la o interfață la cealaltă dacă trebuie efectuată această operație pentru a livra pachetul la destinație. Cu alte cuvinte, gazda cu două plăci de rețea funcționează ca un ruter. Această funcție de rutare se numește în mod obișnuit *retransmisie IP* (*IP forwarding*) și trebuie dezactivată dacă doriți să folosiți calculatorul ca o componentă a firewall-ului.

FIGURA 4.2

Pentru a media traficul de rețea între rețeaua LAN proprie și Internet, poate fi utilizată o gazdă cu două plăci de rețea.



Atunci când introduceți o gazdă cu două plăci de rețea între rețeaua LAN proprie și Internet, calculatoarele client din rețeaua LAN nu pot fi găsite direct din Internet. Pachetele de rețea care sosesc de la clienții din rețeaua LAN printr-o interfață sunt controlate de software-ul intermediar de aplicație care rulează pe calculatorul cu două plăci de rețea. Software-ul intermediar determină dacă solicitarea clientului este permisă și apoi trece la îndeplinirea cererii clientului, trimițând pachetele la interfața externă. Dacă situl dumneavoastră are cerințe ridicate de securitate, nu este recomandat să utilizați un calculator gazdă cu două plăci de rețea ca unică protecție împotriva amenințărilor dinspre Internet. Sistemele de operare pentru calculatoare sunt produse foarte complexe și este foarte dificil de garantat în mod absolut că nu există breșe legate de securitate. De exemplu, Windows NT este compus efectiv din milioane de linii de cod. Oricând poate fi

descoperită o nouă eroare de programare care poate fi exploatată pentru a compromite securitatea sistemului dumneavoastră. Trebuie să păstrați actualizate recomandările de securitate puse la dispoziție de furnizori și să obțineți noile petice sau actualizările pentru a rezolva orice nouă problemă descoperită.

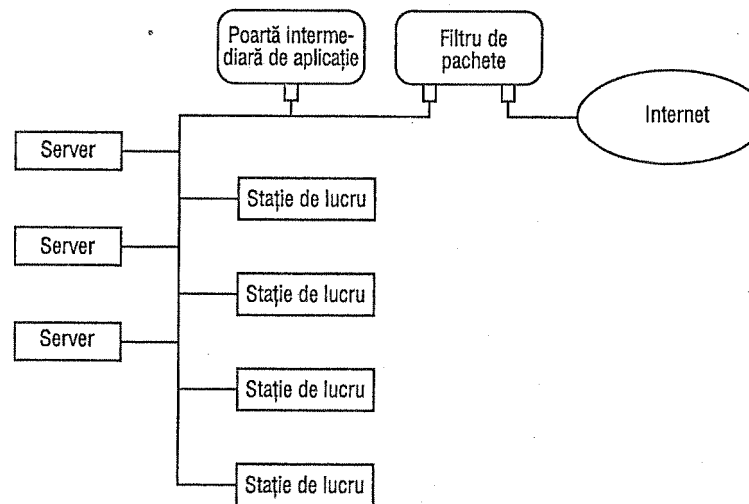
O altă diferență între utilizarea unei gazde cu două plăci de rețea și un ruter cu filtrarea pachetelor este aceea că gazda cu două plăci de rețea operează în mod obișnuit ca un server intermediar de aplicație, și nu ca un filtru de pachete. În loc să folosească o bază de reguli pentru a lua decizii cu privire la ce pachete să retransmită între interfețe, o gazdă cu două plăci de rețea rulează una sau mai multe aplicații intermediare.

Utilizarea unei gazde ecranate

Arhitectura de firewall cu gazdă ecranată are avantajul că posedă atât funcțiile de protecție ale unui filtru de pachete, cât și pe cele ale unei porți intermediare de aplicație. În această configurare, prezentată în figura 4.3, pentru conectarea la Internet este folosit un filtru de pachete, în timp ce un server intermediar este utilizat pentru a oferi servicii clienților din rețeaua LAN internă.

FIGURA 4.3

Un firewall de tip gazdă ecranată oferă atât protecția unui filtru de pachete, cât și protecția unei porți intermediare de aplicație.



Observați că serverul intermediar din această imagine nu folosește cele două interfețe de rețea. Filtrul de pachete este configurat astfel încât traficul care ajunge din Internet îi este permisă trecerea numai dacă este destinat serverului intermediar care se găsește în zona protejată. Același lucru este valabil pentru clienții din rețeaua LAN internă. Cu toate că serverul intermediar și clienții acestuia sunt conectați la aceeași subrețea și este posibil ca o stație de lucru client să trimită pachete direct la filtrul de pachete, acestea sunt respinse. Filtrul de pachete nu permite decât comunicațiile înspre rețeaua LAN care sunt destinate serverului intermediar și nu acceptă decât pachetele transmise în exterior care provin de la serverul intermediar.

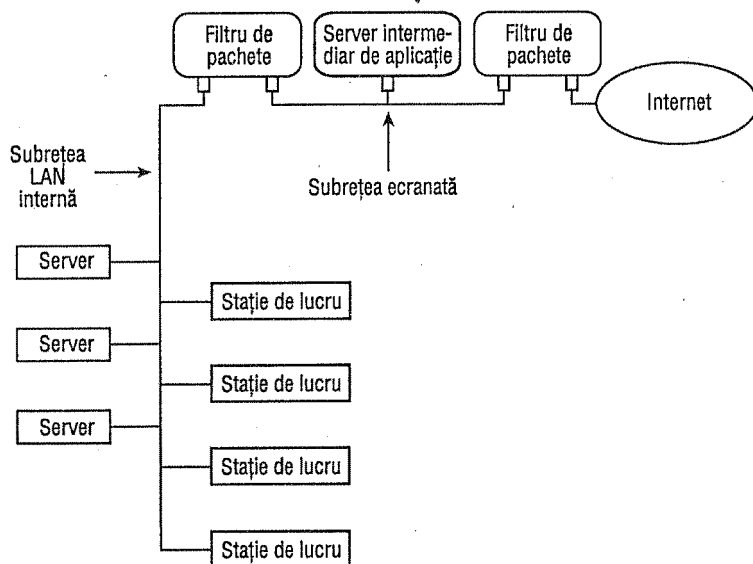
Desigur, toate acestea depind de configurarea corectă a filtrului de pachete. Cu toate că este imposibil ca pachetele să circule între Internet și rețeaua LAN cu un serviciu intermediar atunci când este folosită o gazdă cu două plăci de rețea, limitarea nu se aplică și în acest caz. De exemplu, pot fi servicii pe care trebuie să le utilizați, însă pentru care nu există aplicație intermediară. În această situație, este simplu să configurați filtrul de pachete pentru a permite ca anumite tipuri de pachete să fie rutate între clienții din rețeaua LAN internă și Internet, forțând în același timp toate celelalte servicii să folosească poarta intermediară. Decizia de a permite clienților să comunice direct cu ruterul și să treacă peste serverul intermediar ar trebui să se bazeze pe politica dumneavoastră de securitate.

Utilizarea unei subrețele ecranate pentru a crea o zonă demilitarizată (DMZ)

Ducând conceptul de gazdă ecranată un pic mai departe, puteți probabil să intuiți ce este arhitectura de subrețea ecranată. Și în acest caz este folosit un filtru de pachete pentru a oferi primul nivel de securitate între rețeaua LAN și Internet. Însă în figura 4.4 puteți vedea că la configurație a fost adăugat un alt ruter.

FIGURA 4.4

O arhitectură de subrețea ecranată folosește două filtre de pachete pentru a izola rețeaua LAN de Internet.



Această combinație de rutere creează un segment suplimentar de rețea între Internet și rețeaua dumneavoastră locală. Ruterul care se conectează la Internet operează într-un mod asemănător cu un ruter dintr-o arhitectură cu gazdă ecranată. Acest ruter permite efectuarea comunicațiilor dinspre exterior cu anumite gazde pe care rulează servere intermediare de aplicație. Clienții din rețeaua LAN internă comunică în continuare cu serverele intermediare de aplicație, care sunt responsabile să acționeze în numele clientului în relația cu serverele care se găsesc în Internet. Al doilea ruter, care conectează rețeaua

LAN cu segmentul ecranat de rețea, oferă un nivel suplimentar de securitate, deoarece tot traficul care circulă între clienții din rețeaua LAN și serverele intermediare trebuie să treacă mai întâi prin acest ruter. Pentru a funcționa corect, ruterul extern este configurat astfel încât să permită traficul între un server intermediar din subrețeaua ecranată și rețeaua externă. Ruterul intern permite doar traficul între calculatorul client intern și un server intermediar din subrețeaua ecranată.

Pentru a defini subrețeaua ecranată care se găsește între rețeaua LAN și Internet, este folosit uneori termenul de zonă demilitarizată (demilitarized zone, sau DMZ). În figura 4.4 există un singur server intermediar în zona DMZ. De asemenea, observați că acesta nu are două plăci de rețea. Ruterul situat la limita zonei DMZ garantează că nici un fel de trafic de rețea din Internet nu poate circula direct către calculatoarele din rețeaua LAN, astfel încât serverul intermediar nu trebuie să asigure această funcție. Serverul intermediar nu are nevoie decât de un singur adaptor de rețea pentru a comunica fie cu clienții din rețeaua LAN internă, fie cu ruterul extern.

Există încă un avantaj al utilizării unei zone DMZ în configurația de firewall. Atunci când folosiți un calculator gazdă cu două plăci de rețea ca server intermediar, vă confrunțați inevitabil cu o oarecare încetinire a traficului de rețea între rețeaua LAN internă și Internet. Aceasta se datorează faptului că un calculator și sistemul de operare care rulează pe el nu sunt proiectate să optimizeze comunicațiile prin rețea. Un calculator trebuie să execute numeroase activități, cum ar fi rularea aplicațiilor utilizator și gestionarea dispozitivelor periferice, cum ar fi tastatura sau o imprimantă. Un ruter însă, este proiectat pentru viteză. Un ruter nu trebuie să se preocupe de organizarea în cozi a solicitărilor de acces la disc, de rularea programelor sau de afișarea unor imagini cu rezoluție ridicată pe un monitor. Ruterul monitorizează interfețele de rețea care îi sunt atașate și face tot ce poate pentru a decide cum să livreze pachetele către destinațiile lor.

În figura 4.5, puteți vedea că zona DMZ poate fi un loc în care sunt conectate mai multe servere intermediare. Prin utilizarea mai multor calculatoare în acest scop, posibil câte un calculator separat pentru fiecare serviciu asigurat, veți descoperi că activitățile de gestionare sunt mult mai puțin complicate. Dacă utilizatorii din rețeaua dumneavoastră folosesc mult serviciile care trebuie să circule între serverele intermediare, întrebuintarea mai multor servere va asigura, de asemenea, un serviciu mai rapid și mai eficient decât utilizarea unui singur calculator pentru rularea tuturor serviciilor.

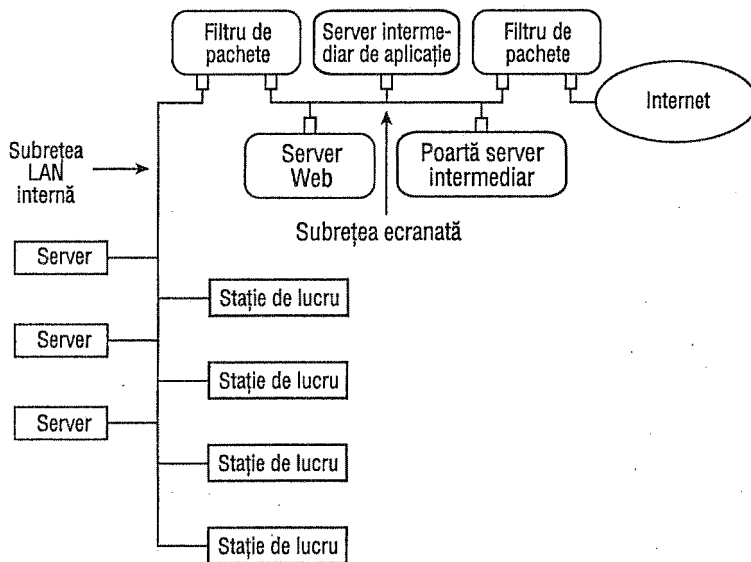
Mai există și alte tipuri de gazde care ar trebui luate în considerare pentru plasarea în zona demilitarizată. De exemplu, dacă gestionați propriul server Web, ați putea să îl conectați direct la Internet și să vă bazați pe mecanismele de securitate ale calculatorului pentru a-l proteja de un posibil atac. Însă dacă plasați serverul Web în zona DMZ, puteți să îi îmbunătățiți mult securitatea. Ruterul de filtrare a pachetelor care se găsește între zona demilitarizată și Internet ar putea fi configurat pentru a permite traficul Web HTTP cu serverul Web, însă în același timp ar putea să interzică traficul FTP. Ruterul intern, care conectează zona DMZ la rețeaua LAN, poate fi configurat astfel încât echipa de dezvoltare Web să poată folosi protocolul FTP pentru a transfera fișiere pe serverul Web.

Un alt candidat excelent pentru plasarea în zona demilitarizată este stiva de modemuri (modem pool). Dacă faceți cheltuieli pentru stabilirea și gestionarea unui firewall, nu ar fi o prostie instalarea de modemuri pe calculatoarele situate în rețeaua LAN? Un modem pe unul dintre sistemele desktop ale utilizatorilor dumneavoastră oferă o intrare secretă în

rețeaua LAN și creează un punct critic de defectare pentru tot sistemul de securitate. *Securitatea rețelei dumneavoastră este la fel de bună ca cea mai slabă legătură din rețea!* Cu toate că ați putea impune o politică severă cu protecție prin parole în situl propriu și v-ați putea gândi că nu există nici o șansă ca un cont de utilizator să fie compromis vreodată, chiar merită să riscați? Dacă ați concediat vreodată un salariat în condiții nu tocmai ideale, sunt sigur că veți înțelege ce am vrut să spun. Chiar dacă puteți să dezactivați cu ușurință contul de utilizator al angajatului astfel încât acesta să nu poată să se conecteze la rețea prin mașina desktop, nu aveți garanția că acest fost angajat nu a descoperit parola pentru alte conturi.

FIGURA 4.5

În zona demilitarizată (DMZ) puteți să plasați mai multe servere intermediare, precum și alte tipuri de servere.



Utilizarea gazdelor bastion și a gazdelor de sacrificiu

Atunci când utilizați o arhitectură cu subrețea ecranată și plasați mai multe servere intermediare în zona DMZ creată, ar trebui să fie evident faptul că mașinile pe care rulează aplicațiile intermediare trebuie să fie securizate la un nivel ridicat. În timp ce calculatoarele client din rețeaua LAN internă sunt protejate de conexiuni directe din Internet, serverele intermediare sunt proiectate special să accepte acest tip de trafic. Chiar dacă un filtru de pachete asigură o oarecare protecție pentru serverele intermediare, nu poate garanta că nimic nu le poate face rău. Astfel, este important să vă concentrați pe mecanismele de securitate puse la dispoziție de sistemul de operare al calculatorului pentru a fi sigur că ați făcut tot ce este posibil pentru a le face capabile să reziste atacurilor provenite din surse răuvoitoare din Internet.

Vezi și

➤ Pentru mai multe informații despre programe de securitate, vezi anexa B, „Alte instrumente de securitate pe care le puteți folosi”.

Termenul *gazdă bastion* (*bastion host*) este utilizat pentru a identifica un calculator gazdă pregătit special pentru acest tip de activitate. Gazda bastion a fost întărită prin eliminarea aplicațiilor și serviciilor care nu sunt necesare și prin utilizarea atenției instrumentelor de securitate oferite de sistemul de operare de bază. Deoarece calculatorul gazdă bastion este mai expus la Internet decât clienții din rețeaua LAN internă, trebuie să folosească orice smecherie posibilă pentru a impune securitatea proprie bazată pe gazdă.

Spre deosebire de stațiile de lucru sau serverele din rețeaua LAN internă, gazda bastion este expusă la atacuri din partea posibiloare răufăcătoare din Internet.

Deoarece gazda bastion se găsește în zona DMZ, mecanismele de securitate ale sistemului de operare sunt deosebit de importante pentru succesul său.

Subrețele ecranate multiple

Puteți să extindeți conceptul de subrețea ecranată prin crearea de mai multe subrețele ecranate plasate între rețeaua dumneavoastră LAN și Internet. De exemplu, în loc să folosiți doar două rutere pentru a crea o singură subrețea ecranată, puteți să utilizați trei rutere pentru a crea două subrețele. Subrețeaua ecranată situată mai aproape de exterior este cea mai vulnerabilă și poate fi folosită pentru gazdele care rulează servicii în care nu se poate avea ușor încredere sau care nu operează la fel de sigur cum v-ar plăcea dumneavoastră. În subrețeaua ecranată din interior, puteți să plasați gazde pe care rulează servicii ce au nevoie de protecție suplimentară.

Pentru ca acest concept să funcționeze, este important să rețineți că nu configurați toate ruterele cu aceleași reguli de filtrare a pachetelor. Dacă ați procedat astfel, trecerea peste al doilea ruter nu ar fi mai dificilă ca trecerea peste primul ruter și așa mai departe.

De asemenea, este o practică uzuală folosirea de produse firewall diferite (filtru de pachete sau intermediar de aplicație) în subrețele ecranate diferite. De ce? Dacă hackerul a fost capabil să compromită o componentă a firewall-ului, sarcina sa devine mai dificilă dacă trebuie să o ia de la început atunci când încearcă să treacă peste următoarea componentă.

Vezi și

➤ O discuție detaliată despre utilizarea unei gazde bastion poate fi găsită în capitolul 6, „Utilizarea unei gazde bastion”.

Un alt tip de sistem pe care puteți să îl plasați în zona DMZ este, într-un fel, opusul gazdei bastion. O *gazdă de sacrificiu* (*sacrificial host*) este un calculator utilizat pentru a ispiți hackerii aflați în căutare. În loc să încerca să țină departe un potențial răufăcător, calculatorul gazdă de sacrificiu permite pătrunderea acestora și, în majoritatea cazurilor, le urmărește pașii, înregistrând informații care ulterior ar putea fi utile pentru depistarea lor sau pentru o mai bună securizare a rețelei dumneavoastră. O altă caracteristică utilă a folosirii acestui tip de gazdă este aceea că poate să țină hackerii ocupați, astfel încât ei nu încearcă să afle mai mult și nu ajung să localizeze gazde mai importante din rețeaua dumneavoastră în care să încerce să pătrundă forțat.

Crearea unei gazde de sacrificiu nu trebuie să fie o operație costisitoare. Deoarece calculatorul nu va fi folosit pentru programare, nu trebuie să selectați un sistem cu cea mai rapidă unitate CPU sau cu un alt echipament superior, cum ar fi un monitor cu rezoluție ridicată sau discuri cu o capacitate extinsă de stocare. Puteți să reciclați un calculator mai vechi căruia nu mai aveți ce utilizare să îi dați. Este important să configurați calculatorul astfel încât să nu fie prea dificil de compromis, dar totuși suficient de dificil pentru a ține hackerul ocupat, astfel încât să puteți începe să îl depistați.

Monitorizați toate gazdele care se găsesc în zona DMZ

Deoarece o gazdă bastion se găsește în mod obișnuit în zona demilitarizată, acesta este calculatorul cel mai expus la atacuri. Cu toate că puteți lua măsuri extreme pentru a proteja gazda bastion prin eliminarea serviciilor și a conturilor de utilizator care nu mai sunt necesare și prin utilizarea tuturor mecanismelor de securitate ale sistemului, nu ar trebui niciodată să presupuneți că acest calculator este complet sigur. Astfel, trebuie să revedeți regulat toate fișierele jurnal produse de sistemul de operare sau de software-ul intermediar, astfel încât să puteți detecta orice intruziune nedorită înainte să devină o problemă majoră. Pentru sistemele UNIX, puteți să folosiți un produs cum ar fi Tripwire. Acest program utilizează rezumate criptografice ale fișierelor de sistem importante pentru a detecta dacă au fost efectuate modificări. Dacă un intrus a pătruns într-o gazdă bastion și a plantat un virus de tip cal troian sau a modificat un fișier important, în mod normal acest program îl detectează.

Puteți să descărcați o versiune sursă deschisă a programului Tripwire de la adresa <ftp://coast.cs.server.purdue.edu/pub/COAST/Tripwire>. O versiune comercială a produsului Tripwire poate fi achiziționată de la firma Tripwire Security Systems Inc., care poate fi găsită la adresa www.tripwiresecurity.com.

Raportarea incidentelor și răspunsuri

O politică bună de securitate a sitului vă va proteja rețeaua numai dacă impuneți aplicarea politicii. Simpla creare a unui document scris și completarea acestuia nu vă apără de nimic. Pentru a face politica funcțională, trebuie să dezvoltați metode de monitorizare a utilizării calculatoarelor și a rețelei și să veniți cu acțiuni specifice care vor fi aplicate atunci când politica este violată.

Multe produse de tip firewall pot fi configurate pentru a declanșa o alarmă sonoră atunci când au loc acțiuni suspecte. De asemenea, majoritatea acestor produse creează fișiere jurnal care pot fi revăzute periodic. Decideți din timp cum veți reacționa la anumite alarme și creați proceduri care pot fi folosite pentru documentarea problemei și remediarea daunelor. Este aproape imposibil să anticipați fiecare tip de breșă de securitate care ar putea apărea în rețeaua dumneavoastră. Ca urmare, procedurile ar trebui să fie măsuri pe care să le puteți modifica și completa pe măsură ce apar noi probleme.

De exemplu, atunci când revedeți un fișier jurnal care conține conturile de utilizator care au fost folosite pentru a deschide sesiuni Telnet pe un server, descoperiți că un cont de utilizator pe care l-ați crezut șters există în continuare și este folosit pentru infiltrarea în rețeaua dumneavoastră. Ce ar trebui să faceți? Câteva operații imediate ar putea fi:

- Schimbarea parolei pentru contul de utilizator suspectat.
- Deconectarea serverului sau a stației de lucru compromise de la rețea.
- Deconectarea rețelei de lumea exterioară prin oprirea ruterului, dacă descoperiți că au fost compromise mai multe calculatoare.

În loc să schimbați parola pentru contul de utilizator, ați putea să ștergeți contul de utilizator astfel încât să nu mai existe nici o șansă să fie folosit în viitor pentru o nouă pătrundere în sistem. Însă, deoarece acest cont este un punct comun de referință între dumneavoastră și persoana răuvoitoare care a pătruns în rețeaua dumneavoastră, s-ar putea să fie mai bine să schimbați parola și apoi să monitorizați activ situația, astfel încât să puteți aduna informații suplimentare care pot fi folosite pentru identificarea și depistarea acelei persoane.

După ce ați reacționat la o breșă în securitatea sistemului dumneavoastră și ați rezolvat-o efectiv, luați în considerare alte operații care trebuie efectuate pentru a determina dimensiunea pagubelor, dacă există, și ce aveți de făcut pentru a le remedia. Dacă a fost modificată o bază de date, doriți să refaceți fișierele de pe o copie de siguranță? Dacă da, cât de departe trebuie să mergeți înapoi în secvența de salvări de siguranță pentru a fi sigur că aveți fișiere care nu au fost corupte? Cum recreați înregistrările pentru informațiile bune care au fost introduse de utilizatorii dumneavoastră între momentul salvării de siguranță și cel al apariției breșei de securitate? În funcție de tipul de informații, există probleme juridice pe care trebuie să le luați în calcul?

Dacă vă gândiți din timp la aceste lucruri și creați proceduri scrise de raportare și răspuns la incidente, vă veți da seama că sarcina dumneavoastră va fi mult mai ușoară în cazul în care se întâmplă ceva.

Ce este o gazdă de sacrificiu?

În acest capitol, am definit o gazdă de sacrificiu ca fiind un calculator pe care sperați că un hacker va încerca să îl atace. În anumite lucrări, termenul este folosit pentru a descrie orice calculator gazdă care se găsește direct în Internet sau în zona DMZ, deoarece aceste calculatoare sunt cel mai ușor de atacat.

Păstrarea la zi a recomandărilor de securitate

Gestionarea celor mai multe aplicații obișnuite de calculator, cum ar fi un program de prelucrare de texte sau un browser Internet, presupune de obicei citirea documentului și efectuarea unor activități de rutină. Gestionarea unui firewall nu este la fel de simplă. Pe lângă instalarea și configurarea firewall-ului, ar trebui să folosiți toate mecanismele furnizate pentru înregistrarea în jurnale, alarmare și avertizare. Verificarea zilnică a fișierelor jurnal ar trebui să devină o obișnuință. Atunci când stabiliți alarme sau alte mecanisme de avertizare, asigurați-vă că sunt configurate astfel încât rapoartele să ajungă la cineva care este în măsură să răspundă într-o perioadă scurtă de timp.

Întreținerea sistemului de securitate nu este o activitate statică. Este un proces continuu de evaluare și răspuns la erorile de programare software și la problemele noi, pe măsură ce sunt descoperite. Dacă ați achiziționat un produs firewall comercial, nu uitați să citiți recomandările referitoare la securitate oferite de furnizor imediat ce le primiți. Noile petice software trebuie evaluate și instalate periodic dacă sunt potrivite pentru rețeaua dumneavoastră și pentru software-ul sau firewall-ul instalat în rețea.

În plus, există în Internet numeroase resurse care pot fi folosite pentru a vă ajuta să fiți permanent la curent cu situațiile noi care pot provoca o compromitere a sistemului de securitate atașat rețelei dumneavoastră. În anexa C, „Resurse suplimentare”, veți găsi o listă cu multe situri utile, cum ar fi FIRST (Forum of Incident Response and Security Teams) și CERT (Computer Emergency Response Team). Aceste organizații, împreună cu altele amintite în lista din anexă, au și liste poștale la care vă puteți abona, astfel încât să fiți permanent la curent cu noutățile apărute.

Configurarea unui firewall nu este ceva ce faceți și uitați. Este un proces continuu de monitorizare, evaluare și actualizare.

Păstrați fișierele jurnal cel puțin un an!

Fișierele jurnal, indiferent că sunt produse de sistemul de operare, de un software de aplicație sau de firewall, pot fi o armă foarte utilă pentru depistarea hackerilor și determinarea modului în care a fost compromis un sistem de calculator sau de rețea. Deoarece un virus de calculator sau un alt program dăunător, cum ar fi un cal troian, poate să se ascundă în rețeaua dumneavoastră mai multe luni până să fie activat, este recomandat să păstrați fișierele jurnal o perioadă mai îndelungată. Este ușor să scrieți un fișier script (sau o procedură de comandă, în funcție de sistemul de operare) care să arhiveze regulat fișierele jurnal pe un alt sistem sau pe un dispozitiv pentru salvări de siguranță. Păstrați aceste fișiere jurnal cel puțin un an înainte să reciclați suporturile pentru salvările de siguranță.

Rezumat

Înainte de a începe să construiți (sau să cumpărați) un firewall, trebuie să înțelegeți bine politicile de securitate impuse în situl dumneavoastră. Dacă nu ați scris încă politici de securitate, ar trebui să începeți să o faceți înainte chiar de a începe să vă gândiți la un firewall. Politica de securitate trebuie să fie suficient de flexibilă pentru a permite utilizatorilor dumneavoastră să își îndeplinească sarcinile de serviciu, dar totuși suficient de restrictivă pentru a împiedica să fie compromisă rețeaua de calculatoare. Nu uitați că o politică de securitate excesiv de severă poate avea două consecințe nedorite: utilizatorii nu își îndeplinesc sarcinile și, în plus, găsesc alte mijloace de a submina regulile stabilite de dumneavoastră. Politica de securitate pe care o stabiliți trebuie să fie corectă și să fie dezvoltată pe baza informațiilor primite de la departamentele și utilizatorii pe care îi va afecta.

Modul în care proiectați firewall-ul depinde de câțiva factori, între care se numără gradul de securitate necesar sitului dumneavoastră, ca și bugetul alocat pentru această activitate. Cu toate că un simplu ruter cu filtrarea pachetelor este ieftin – este chiar gratuit dacă aveți deja un ruter prin care vă conectați la Internet – nu oferă decât un nivel minimal de protecție. Un proiect mai complex, care folosește mai multe subrețele ecranate, poate deveni rapid o soluție scumpă, atât în ceea ce privește crearea, cât și în ceea ce privește întreținerea.

În final, securitatea pe care o aveți pentru rețeaua dumneavoastră este bună atâta timp cât este actualizată. Zilnic sunt descoperite noi erori de programare în aplicațiile software și în sistemele de operare. Dacă nu cunoașteți ultimele recomandări referitoare la securitate, s-ar putea să nu fiți protejat de aceste erori.

Capitolul 5**Filtrarea pachetelor**

- Prima linie de apărare
- Informațiile din antetul IP care pot fi folosite pentru filtrarea pachetelor
- Informațiile de antet TCP și UDP
- Pachete ICMP
- Operarea independent de stare în comparație cu inspectarea dependentă de stare
- Filtre de pachete hardware și software
- Avantajele și dezavantajele filtrelor de pachete

Prima linie de apărare

Ruterele cu ecranare au reprezentat primele firewall-uri. De obicei vă gândiți la un ruter ca la un dispozitiv de rețea a cărui sarcină este de a lua decizii în ceea ce privește modul de retransmitere a unui pachet astfel încât acesta să poată fi livrat. Adăugarea listelor de control al accesului permite unui ruter să monitorizeze ce pachete au permisiunea să circule prin interfețele sale de rețea. Această metodă simplă de retransmitere sau de respingere a unui pachet pe baza regulilor stabilite de administratorul de rețea reprezintă baza unui filtru de pachete. Ruterul cu ecranare efectuează o funcție de filtrare, astfel încât numai pachetelor care îndeplinesc anumite criterii le este permisă trecerea.

În capitolele anterioare, ați învățat câte ceva despre filtrele de pachete. Cel mai important lucru de care trebuie să vă amintiți este că filtrul de pachete ar trebui să nu fie singura metodă pe care o folosiți pentru construirea unui firewall. Filtrul ar trebui considerat primul dispozitiv pe care îl utilizați și ar trebui susținut de unul sau mai multe servere intermediare și, în unele arhitecturi, de un alt ruter.

Unde trebuie folosite filtrele de pachete

În figura 5.1, puteți vedea trei scenarii diferite care întrebunțează un ruter pentru a filtra pachetele înainte ca acestea să fie distribuite în rețeaua LAN. În fiecare dintre cele trei cazuri, ruterul cu ecranare este poziționat cel mai aproape de conexiunea la Internet. Aceasta înseamnă că se găsește la marginea rețelei și acționează ca un *portar* (*gatekeeper*).

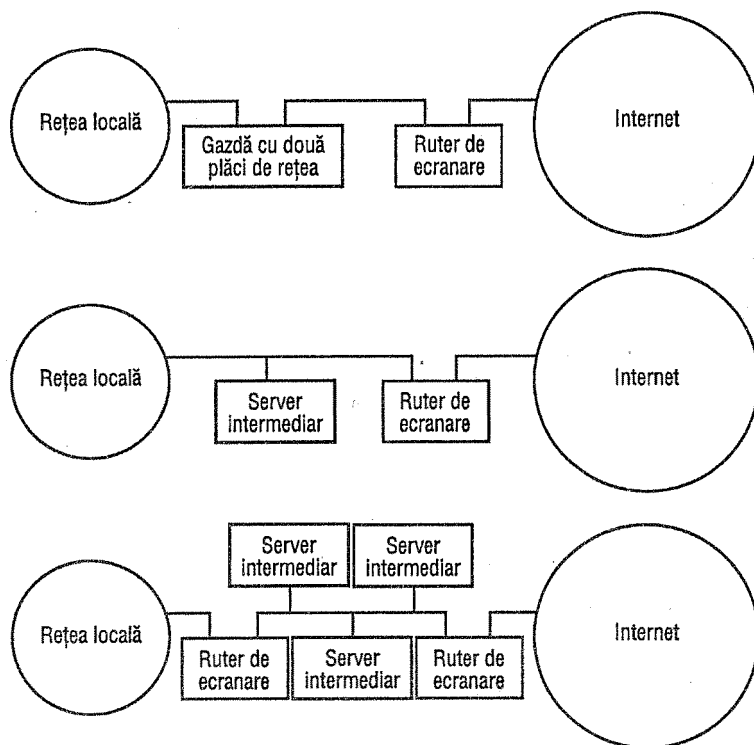
În prima situație, ruterul ecranează pachetele înainte ca acestea să fie livrate unui calculator gazdă cu două plăci de rețea. Ruterul acționează ca un filtru de pachete. Calculatorul gazdă cu două plăci de rețea a fost configurat într-un mod foarte sigur ca o gazdă bastion. Serviciile și conturile de utilizator care nu sunt necesare au fost eliminate de pe acest calculator, iar sistemul de operare a fost modificat astfel încât să nu existe pachete care să fie retransmise automat de la o interfață la cealaltă. Rezultatul acestor modificări este acela că nici un pachet IP nu are permisiunea să circule direct din rețeaua locală către Internet. Software-ul de pe gazda cu două plăci de rețea (intermediar de aplicație) este responsabil pentru discuțiile cu clienții din rețeaua internă și interacțiunea cu serverele din Internet în numele acelor clienți.

Vezi și

➤ Pentru mai multe informații despre configurarea unei gazde bastion, vezi capitolul 6, „Utilizarea unei gazde bastion”.

FIGURA 5.1

Unul dintre elementele componente ale firewall-ului ar trebui să fie un ruter cu ecranare folosit ca filtru de pachete.



În al doilea caz, puteți vedea că nu este absolut necesar să folosiți un calculator cu două plăci de rețea pentru găzduirea serviciilor intermediare. O conexiune este suficientă. Însă în acest tip de configurare, este important ca ruterul să fie configurat astfel încât să permită pachetelor să circule între Internet și serverul intermediar și să nu permită trecerea nici unui trafic direct din Internet către rețeaua LAN internă. Acest model este denumit în

mod obișnuit *configurație cu gazdă ecranată (screened-host configuration)*. Este considerat mai puțin sigur decât utilizarea unei gazde cu două plăci de rețea pentru aplicațiile intermediare. Aceasta întrucât clienții din rețeaua internă trebuie să fie configurați corect, astfel încât să trimită pachete către serverul intermediar și să nu încerce să comunice direct cu serverele din Internet.

Din punctul de vedere al securității, este mai ușor pentru dumneavoastră să controlați configurația de securitate pe un calculator cu două plăci de rețea decât pe fiecare client din rețeaua proprie. Chiar dacă aveți reguli și proceduri operaționale care controlează modul în care sunt configurați clienții, un angajat răuvoitor poate oricând să reconfigureze propria stație de lucru în scopul trecerii peste serverul intermediar. De asemenea, un program de tip cal troian plantat de un intrus poate să procedeze la fel. Forțând întregul trafic IP să circule prin calculatorul cu două plăci de rețea, dispuneți de un punct unic de verificare pentru a controla accesul la Internet.

A treia configurație, care implică două rutere, creează o subrețea între Internet și rețeaua LAN internă și este cunoscută sub numele de *subrețea ecranată (screened subnet)*. Calculatoarele gazdă care se găsesc în subrețeaua ecranată sunt protejate de ruterul conectat la Internet. Pentru a apăra clienții din rețeaua LAN internă, este folosit un alt ruter. Atunci când utilizați o subrețea ecranată, puteți să plasați în aceasta una sau mai multe gazde. Deoarece aveți un ruter suplimentar pentru ecranarea traficului înainte ca acesta să ajungă în rețeaua LAN internă, puteți să plasați în subrețeaua ecranată câteva calculatoare care să nu fie neapărat configurate la fel de sigur ca o gazdă bastion întărită. De exemplu, pe lângă serverele intermediare, subrețeaua poate să mai includă servere Web, stive de modemi și alte servere.

Vezi și

➤ Pentru mai multe informații despre utilizarea unei gazde cu două plăci de rețea, ca și despre gazde ecranate și subrețele ecranate, vezi capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”.

Scopul acestei treceri în revistă este de a înțelege că modul în care configurați un filtru de pachete depinde, până la urmă, de funcția pe care i-o acordați. Dacă folosiți o configurație similară cu primul caz, ruterul de ecranare poate fi configurat pentru a filtra traficul nedorit, însă gazda cu două plăci de rețea este responsabilă pentru orice interacțiune pe care clienții din rețeaua LAN internă o au cu serverele din afara rețelei. În acest caz, s-ar putea să nu fiți nevoit să folosiți un set de reguli complicate pentru configurarea ruterului.

În al doilea caz, ruterul trebuie să fie securizat pentru a preveni pătrunderea pachetelor care nu sunt adresate serverului intermediar. În ultimul caz, ruterul cel mai apropiat de Internet poate fi configurat într-o manieră mai lejeră, însă ruterul apropiat de rețeaua LAN internă trebuie să fie foarte securizat, permițând doar comunicații între serverele intermediare (sau alte gazde) și clienții din rețeaua LAN internă. Această situație poate necesita o serie de reguli mai complexe. De exemplu, majoritatea clienților dumneavoastră trebuie să comunice cu un server intermediar, astfel încât le puteți pune la dispoziție acces Web sau alte servicii populare. Dacă aveți un server Web situat în subrețeaua ecranată, veți dori să configurați ruterul astfel încât numai câțiva clienți să fie capabili să comunice cu acesta, și anume stațiile de lucru ale utilizatorilor care răspund de producerea paginilor Web pe care le oferiți în Internet.

O altă situație de luat în considerare pentru filtrele de pachete presupune folosirea mai multor firewall-uri într-o rețea mare pentru a separa rețeaua de calculatoare a unei companii în componente funcționale. De exemplu, este posibil ca departamentul de cercetare al unei companii să aibă cerințe de securitate și de conectivitate la Internet diferite de cele ale departamentelor de contabilitate și producție. Ca urmare, ar putea fi util să folosiți un firewall între rețelele LAN care formează aceste departamente. În această situație, regulile dumneavoastră sunt probabil mai ușor de configurat, deoarece aveți deja un firewall la perimetrul rețelei care se ocupă de relația cu exteriorul.

În orice caz, nu uitați că filtrul de pachete, indiferent dacă este un ruter sau un calculator gazdă cu software de filtrare a pachetelor, trebuie configurat în funcție de modul de configurare a firewall-ului. Pentru a crea un filtru de pachete, nu există un răspuns simplu la întrebarea „Ce reguli trebuie să stabilesc?”. Acesta depinde de serviciile pe care doriți să le puneți la dispoziție, de utilizatorii cărora le oferiți aceste servicii și de modul în care doriți să le configurați.

Crearea de reguli pentru filtrarea pachetelor

Pentru a decide cum veți stabili regulile pentru un filtru de pachete, la început luați hotărâri referitoare la următoarele aspecte:

- Ce servicii doriți să oferiți în rețea și în ce direcție (din interior către exterior sau din exterior către interior) doriți să funcționeze?
- Doriți să limitați abilitatea vreunui calculator gazdă intern de conectare la serviciile Internet?
- Există gazde sigure în Internet care vor avea nevoie de un anumit tip de acces în rețeaua dumneavoastră internă?

Tipurile de informații pe care le puteți folosi pentru a crea reguli variază puțin de la un produs la altul, însă în general veți vedea că următoarele elemente sunt cele mai utile:

- **Interfața și direcția** – Dacă un pachet părăsește sau ajunge în rețeaua dumneavoastră și prin ce interfață trece pentru aceasta.
- **Adresele IP sursă și destinație** – Trebuie să fiți capabil să verificați atât locul de unde pretinde un pachet că provine (adresa IP sursă), cât și locul în care dorește să ajungă (adresa IP destinație).
- **Opțiunile IP** – Trebuie să puteți să verificați acest câmp, în special pentru a împiedica rutarea la sursă.
- **Protocolul de nivel mai înalt** – Tipul de protocol care folosește pachetul IP. De exemplu, TCP sau UDP.
- **Pentru pachetele TCP, bitul ACK** – Verificarea acestui bit vă poate ajuta să determinați dacă se face o încercare de stabilire a unei conexiuni și în ce direcție.
- **Dacă este ICMP (Internet Control Message Protocol), tipul de mesaj** – Puteți să împiedicați anumite încercări de căutare a unor informații despre rețeaua dumneavoastră.
- **Porturile sursă și destinație pentru pachetele TCP și UDP** – Aceste informații vă pot ajuta să stabiliți ce servicii sunt folosite.

Atunci când creați reguli pentru un filtru de pachete, există mai multe convenții importante care trebuie respectate.

În primul rând, în cazul regulilor folosite pentru a permite sau a interzice accesul într-o gazdă sau rețea, folosiți adresa IP, și nu numele de gazdă sau de domeniu. Deși nu este foarte greu de falsificat o adresă IP sau un nume de gazdă, pentru multe tipuri de atacuri, o adresă IP falsificată nici nu este funcțională, deoarece dacă hackerul se așteaptă să primească un răspuns și utilizează o adresă IP falsificată, el nu va primi răspunsul respectiv fără ceva efort. Falsificarea unui nume de gazdă sau de domeniu este o operație foarte simplă dacă hackerul are acces la baza de date DNS. În acest caz, numele s-ar putea să vă pară familiar, însă adresa pe care o translatează s-ar putea să nu fie cea la care vă așteptați.

Vezi și

➤ Pentru mai multe informații despre falsificarea IP, vezi capitolul 3, „Securitate și Internet“.

Nu returnați toate codurile ICMP prin interfața externă. Ele pot dezvălui informații unui atacator, mai precis ce pachete pătrund în interior și ce pachete nu pătrund. Returnarea codurilor ICMP numai pentru anumite pachete îi poate indica atacatorului că acolo este într-adevăr funcțional un mecanism de filtrare a pachetelor. În această situație, pentru hacker orice informație despre rețeaua dumneavoastră este mai bună decât nimic. Una dintre funcțiile principale ale unui firewall este de a ascunde informațiile despre rețeaua internă. Prin eliminare, un hacker poate afla ce nu funcționează și, eventual, ce funcționează. Dacă nu returnați codurile ICMP, ajutați la limitarea informațiilor disponibile pentru un hacker informat.

Respingeți toate pachetele care pătrund prin adaptorul de rețea extern și pentru care adresa sursă nu poate proveni decât din rețeaua protejată. Aceste pachete sunt probabil de la cineva care încearcă să folosească falsificarea adreselor pentru a depăși sistemul dumneavoastră de securitate. Am discutat anterior despre acest aspect, însă este bine să îl repetăm și aici. Există întotdeauna posibilitatea ca cineva din rețeaua internă să fi creat o altă conexiune la Internet, poate din greșală, dacă un alt ruter a fost configurat greșit sau dacă a fost instalată o linie telefonică fără ca dumneavoastră să știți. Ar trebui ca întotdeauna să fiți conștient de faptul că un firewall nu vă poate apăra de atacuri (sau de prostie) provenite din interior. Nu uitați că monitorizarea regulată și vigilența trebuie întreținute pentru măsurile normale de securitate, cum ar fi cunoașterea componentelor rețelei și a modului în care trebuie configurate.

Servicii periculoase

Unele servicii sunt mai periculoase decât altele. TCP/IP a fost creat înainte ca rețeaua Internet să permită utilizarea în scop comercial și la domiciliu. Era o rețea de rețele între situri academice și militare și câteva companii mari care făceau afaceri cu acestea. Unele aspecte legate de securitate care sunt atât de importante în prezent nici nu erau menționate în perioada în care a fost dezvoltată suita de protocoale TCP/IP sau când au fost create unele dintre cele mai răspândite servicii de rețea. Între serviciile „periculoase” cărora nu ar trebui să le permiteți trecerea prin firewall se numără următoarele:

- **Network File System (NFS)** – Dacă permiteți trecerea acestui tip de trafic prin firewall, este posibil ca cineva din exteriorul rețelei dumneavoastră să fie capabil să monteze un sistem de fișiere din rețeaua internă și să acceseze fișiere și directoare ca și cum ar fi conectat la rețeaua LAN.

- **Network Information Services (NIS)** – Acest serviciu, care era cunoscut înainte sub numele „Yellow Pages”, poate oferi hackerilor informații valoroase, cum ar fi nume de gazde și de utilizatori din rețeaua dumneavoastră.
- **X Windows** – Sunt multe probleme de securitate provocate de folosirea clienților și serverelor X. Pe lângă problemele asociate cu modul în care sunt rulate aplicațiile și privilegiile utilizate, permiterea unei sesiuni X Window poate fi la fel de dăunătoare ca o sesiune Telnet.

Nu uitați să interziceți toate serviciile cu o regulă la sfârșitul propriei liste de reguli. Nu deschideți decât serviciile despre care știți cu siguranță că vor fi folosite de clienții dumneavoastră și numai în direcția sigură pentru serviciul respectiv. Dacă utilizați prin firewall servicii cum ar fi Telnet sau FTP, asigurați-vă că folosiți o versiune care oferă fie o formă de autentificare puternică, fie utilizarea unui serviciu intermediar, așa cum este explicat în capitolul următor.

Informațiile din antetul IP care pot fi folosite pentru filtrarea pachetelor

În general, filtrele de pachete operează numai cu informațiile de antet pe care le găsesc în pachet. Deoarece există mai multe anteturi diferite de protocoale în fiecare pachet, le veți analiza doar pe cele care sunt importante pentru filtrarea pachetelor. Majoritatea filtrelor de pachete nu folosesc informațiile de antet găsite la nivelul de cadru Ethernet. Adresa sursei și alte informații similare sunt puțin folosite, deoarece este vorba fie de o adresă hardware MAC locală pentru un sistem din rețeaua LAN, fie de o adresă a unui ruter responsabil pentru ultimul segment din călătoria unui pachet prin Internet.

În continuare, în stiva de protocoale urmează informațiile de antet pentru pachetul IP. În figura 5.2 puteți vedea că aceste informații sunt foarte limitate în antetul unui pachet IP.

FIGURA 5.2 0 4 8 16 31

Câmpurile din antetul IP pot fi folosite pentru a selecta pachetele în vederea filtrării.

Versiune (4 biți)	IHL (4 biți)	Tip de ser- viciu (8 biți)	Lungime totală (16 biți)	
Identificare (16 biți)			Indicator (3 biți)	Deplasament de fragment (13 biți)
Durata de viață (8 biți)	Protocol (8 biți)		Suma de control a antetului (16 biți)	
Adresa IP sursă (32 de biți)				
Adresa IP destinație (32 de biți)				
Opțiuni, dacă există (variabil)				Completare (variabil)
Date (variabil)				

Ce informații utile poate folosi filtrul de pachete din acest antet?

Există trei informații importante:

- **Adresa IP** – Atât adresa sursă, cât și adresa destinație
- **Protocoale** – Cum ar fi TCP, UDP și ICMP
- **Opțiunile IP** – Cum ar fi rutarea la sursă

Cele mai evidente informații care pot fi utilizate sunt câmpurile cu adresa sursă și adresa destinație. Dacă nu aveți decât un număr limitat de calculatoare gazdă din Internet cărora doriți să le permiteți accesul prin firewall, puteți filtra pachetele sosite pe baza adresei sursă. Același lucru este valabil și în sens invers: puteți filtra pachetele care sosesc din interiorul rețelei dumneavoastră astfel încât numai anumite adrese destinație să aibă permisiunea de trecere prin firewall și mai departe în Internet.

Următorul câmp din antetul IP care poate fi util este câmpul Protocol. Acest câmp definește protocolul pentru care vor fi folosite datele utile din pachet. Acesta poate fi, de exemplu, TCP sau UDP, unul din cele două protocoale de transport principale utilizate în Internet. De asemenea, poate fi și ceva gen ICMP. Ca regulă, respingeți pachetele de la orice protocol care nu este folosit în rețeaua dumneavoastră sau care poate permite unei persoane din afara rețelei să reconfigureze modul în care funcționează rețeaua de calculatoare. De exemplu, printre utilizările protocolului ICMP se numără informarea ruterelor referitor la faptul că o destinație nu poate fi atinsă sau cererea adresată ruterului dumneavoastră de a reconfigura tabelele proprii în vederea schimbării rutei către o anumită rețea. Dacă doriți să citiți lista, folosiți un program motor de căutare pentru a găsi specificațiile RFC 1700.

Informațiile de antet TCP și UDP

Fiecare strat din stiva de protocoale adaugă informații de antet datelor pe care le recepționează de la stratul de deasupra lui. Deoarece protocolul IP este utilizat de alte protocoale, cum ar fi TCP și UDP, vă puteți aștepta ca în interiorul porțiunii de date a pachetului IP să se găsească informații de antet plasate de protocoalele amintite. O parte dintre aceste informații sunt foarte utile pentru filtrarea pachetelor. În figura 5.3 puteți vedea structura antetului TCP. Aceste informații de antet sunt numite uneori *TCP Protocol Data Unit*.

Amintiți-vă că TCP răspunde de stabilirea unei sesiuni sigure, orientate spre conexiune, între două aplicații într-o rețea. TCP recepționează datele (denumite *mesaje*) de la straturile situate deasupra sa în stiva de protocoale, adaugă propriile informații de antet și apoi transmite pachetul către stratul IP, care adaugă la rândul său informațiile proprii de antet. Mesajul trimis către TCP de la aplicații prin stivă în sus este denumit de obicei *flux* de date, deoarece cantitatea de date poate să varieze și nu este limitată la un număr fix de octeți. Protocolul TCP preia aceste mesaje și, dacă sunt prea mari pentru a putea să încapă într-un pachet, le împarte în segmente mai mici și trimite fiecare segment într-un pachet separat. Stratul TCP de la capătul receptor reassemblează aceste mesaje înainte să le transmită mai sus către o aplicație.

Cele mai multe dintre informațiile de antet pe care le-ați analizat pentru antetul IP au fost utilizate pentru rutarea pachetului prin Internet – de exemplu, adresele sursă și destinație.

Informațiile din antetul TCP sunt dedicate altor aspecte, cum ar fi siguranța conexiunii și ordonarea mesajelor transmise. Haideți să trecem în revistă rapid câmpurile folosite de protocolul TCP:

FIGURA 5.3

Câmpurile din antetul protocolului TCP pot fi folosite și pentru filtrarea pachetelor.

Port sursă (16 biți)				Port destinație (16 biți)			
Număr de secvență (32 de biți)							
Număr de confirmare (32 de biți)							
Sumă de control (16 biți)				Window (16 biți)			
Pointer urgent (16 biți)				Opțiuni și completare			

- **Portul sursă** – Acesta este un câmp de 16 biți folosit pentru identificarea portului utilizat de aplicația care trimite datele.
- **Portul destinație** – Acesta este un câmp de 16 biți folosit pentru identificarea portului la care va fi livrat pachetul la capătul receptor al conexiunii.
- **Numărul de secvență** – Acesta este un câmp de 32 de biți folosit pentru a identifica locul în care se găsește un segment într-un mesaj mai mare atunci când mesajul este împărțit în fragmente pentru transmisie.
- **Numărul de confirmare** – Acesta este un câmp de 32 de biți folosit pentru indicarea numărului de secvență care urmează.
- **Deplasamentul datelor** – Este un câmp de 4 biți utilizat pentru a specifica numărul de cuvinte de 32 de biți care formează antetul. Acest câmp este folosit pentru a calcula începutul porțiunii de date a pachetului.
- **Zona rezervată** – Acești 6 biți au fost rezervați pentru o utilizare viitoare și, deoarece nu sunt folosiți niciodată, trebuie să aibă valoarea zero.
- **Indicatorul URG** – Atunci când acest bit are valoarea 1, câmpul denumit Pointer urgent indică o secțiune a zonei de date a pachetului specificată ca „urgent”.
- **Indicatorul ACK** – Acesta este bitul de confirmare. Dacă primește valoarea 1, pachetul este o confirmare. Dacă primește valoarea 0, pachetul nu este o confirmare.

- **Indicatorul PSB** – Dacă primește valoarea 1, acest bit indică o funcție push; în celelalte cazuri, are valoarea 0.
- **Indicatorul RST** – Dacă primește valoarea 1, acest bit este un semnal care indică resetarea conexiunii; în celelalte cazuri, are valoarea 0.
- **Indicatorul SYN** – Dacă primește valoarea 1, acest bit indică faptul că numerele de secvență trebuie sincronizate. Dacă primește valoarea 0, numerele de secvență nu trebuie sincronizate.
- **Indicatorul FIN** – Dacă primește valoarea 1, acest bit specifică faptul că expeditorul a terminat de trimis informațiile. În celelalte cazuri, primește valoarea 0.
- **Window** – Acest câmp de 16 biți este folosit pentru a specifica câte blocuri de date este capabil să accepte în acest moment calculatorul receptor.
- **Suma de control** – Acest câmp de 16 biți este o valoare calculată, utilizată pentru verificarea integrității antetului și a zonelor de date din pachet.
- **Pointerul urgent** – Dacă indicatorul URG este activat, acest câmp de 16 biți indică deplasamentul față de câmpul numărului de secvență din zona de date a pachetului unde sunt stocate datele urgente. Acest câmp nu este folosit de TCP, ci de aplicațiile situate deasupra protocolului TCP în stivă.
- **Opțiuni** – Acest câmp poate avea lungime variabilă și este asemănător cu câmpul de opțiuni din antetul IP. Una dintre funcțiile pentru care este utilizat acest câmp este specificarea dimensiunii maxime a segmentului.

Deoarece câmpul de opțiuni poate varia ca dimensiune, antetul este completat cu biți suplimentari, astfel încât să aibă o dimensiune multiplu de 32.

Având disponibile toate aceste informații, puteți observa că protocolul TCP poate exercita un bun control asupra conexiunii. Însă, prin modificarea unor câmpuri, și hackerii pot exercita un bun control asupra unei conexiuni. De exemplu, prin manipularea biților indicatori ACK și SYN, hackerii sunt capabili să folosească atacuri de tip interzicerea serviciului, denumite inundație SYN. Prin modificarea informațiilor din antetul TCP, în special a numerelor de secvență și de confirmare, este posibilă „deturnarea” unei conexiuni TCP.

FIGURA 5.4

Protocolul UDP folosește un antet mai mic.

Port sursă (16 biți)	Port destinație (16 biți)
Lungime (16 biți)	Sumă de control (16 biți)

Antetul UDP este mult mai mic decât antetul TCP. În figura 5.4 puteți vedea că acest antet

nu include decât patru câmpuri, iar dintre acestea doar două, porturile sursă și destinație, sunt utile pentru filtrarea pachetelor.

UDP este un protocol fără conexiune, care nu garantează livrarea și nu face mai mult decât să trimită datele în rețea.

Porturi și socluri

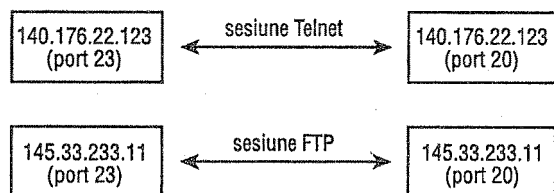
Cele două câmpuri importante din aceste două anteturi utilizate de filtrele de pachete sunt porturile sursă și destinație. Dacă nu ați citit încă introducerea în protocolul TCP din capitolul 2, s-ar putea să vă întrebați pentru ce este folosit un port. Până la urmă, adresele

sursă și destinație din antetul IP sunt utilizate pentru a identifica cele două mașini din rețea care își trimit pachete una alteia. Ca urmare, de ce sunt necesare porturile?

Porturile sunt folosite pentru a identifica punctele finale de aplicație ale conexiunii. Deoarece un anumit calculator poate avea mai multe aplicații care utilizează simultan stiva TCP, trebuie să existe o metodă de diferențiere a pachetelor care lucrează cu aplicații diferite. De exemplu, să presupunem că ați stabilit o sesiune Telnet cu un calculator situat la distanță și vă hotărâți să descărcați un fișier de pe acel calculator. Utilitarul Telnet nu transferă fișiere, astfel că va trebui să deschideți o conexiune FTP. Deoarece adresele sursă și destinație ar trebui să fie aceleași în pachetul IP pentru ambele sesiuni, numerele de porturi sunt utilizate pentru a indica aplicația.

FIGURA 5.5

Un soclu este format dintr-o adresă și un număr de port și identifică în mod unic un punct final al unei conexiuni de rețea.



Atunci când combinați o adresă cu un număr de port, aveți un identificator care poate identifica în mod unic ambele

puncte finale ale unei aplicații. Numele folosit pentru această combinație de numere este *soclu* (*socket*). Soclul este ilustrat în figura 5.5, în care două calculatoare au stabilit două sesiuni de comunicație, una pentru Telnet (portul 23) și cealaltă pentru FTP (portul 20). FTP folosește în realitate două porturi – portul 20 pentru trimiterea datelor și portul 21 pentru schimbul de informații de comandă.

Ar trebui să devină evident pentru dumneavoastră de ce un filtru de pachete găsește utile aceste numere de porturi. În loc să permită sau să interzică pachetele numai pe baza adreselor sursă și destinație – și astfel să permită sau să interzică *toate* comunicațiile – este posibil să permită sau să interzică selectiv *servicii* individuale. Chiar dacă nu doriți ca utilizatorii dumneavoastră să deschidă sesiuni Telnet pe un calculator gazdă situat la distanță (sau invers), nu vă interesează dacă ei schimbă fișiere prin sesiuni FTP anonime. Prin utilizarea numerelor de porturi în regulile de filtrare a pachetelor, puteți permite sau interzice serviciile de rețea unul câte unul.

În implementarea BSD originală a stivei TCP/IP, numerele de porturi din intervalul 0-1023 au fost denumite porturi *privilegiate*. Aceasta înseamnă că urmau să fie folosite de programe care rulează ca root pe o mașină UNIX, iar aceste programe sunt de obicei programele server ale anumitor servicii. Ca urmare a acestei convenții, programele client urmau să aleagă un număr de port mai mare de 1023. Deși această regulă nu a fost standardizată într-un document RFC, este ceva obișnuit ca și alte stive TCP/IP să adere la convenție.

Aceste informații pot fi utilizate cu folos atunci când creați regulile pentru filtrele de pachete. Un filtru de pachete bun vă permite să specificați în regulile pe care le creați atât portul sursă, cât și portul destinație. Unele rutere mai vechi nu permiteau specificarea portului sursă, iar această lipsă putea conduce la breșe foarte mari în securitatea firewall-ului dumneavoastră.

De exemplu, haideți să analizăm câteva mostre de reguli pe care le-ați putea crea pentru a permite conexiuni SMTP către interior și către exterior, astfel încât să poată fi livrată poșta electronică. În primul exemplu, în regulă nu este permis decât portul destinație:

Rule	Direction	Protocol	Source Address	Dest. Address	Dest. Port	Action
1	inbound	TCP	external	internal	25	allow
2	outbound	TCP	internal	external	>=1024	allow
3	outbound	TCP	internal	external	25	allow
4	inbound	TCP	external	internal	>=1024	allow
5	*	*	*	*	*	disallow

În acest exemplu, puteți vedea că regulile 1 și 3 permit conexiuni către și dinspre portul 25, care este portul folosit uzual de protocolul SMTP. Regula 1 permite unei gazde din exterior să trimită o cerere la portul 25 de pe un server din interiorul rețelei dumneavoastră. Regula 2 ar trebui să permită acelui server din rețeaua dumneavoastră să răspundă serverului SMTP, presupunând că folosește un număr de port sursă mai mare de 1023, deoarece regula permite conexiuni la porturi cu valoarea mai mare sau egală cu 1024. Regulile 3 și 4 permit o conexiune SMTP în direcția inversă, în care serverul SMTP din rețeaua LAN internă dorește să realizeze o conexiune la portul 25 de pe un server SMTP care se găsește în rețeaua externă. Ultima regulă, numărul 5, interzice orice altă conexiune. Astfel, s-ar părea că am scris câteva reguli bune care vor proteja rețeaua LAN internă, permițând în același timp conexiuni SMTP în ambele direcții. Corect?

Greșit. Amintiți-vă că atunci când creați un set de reguli pentru un filtru de pachete, trebuie să analizați toate regulile împreună, și nu doar câte una sau câte două. În exemplul pe care l-am discutat, regulile 2 și 5 permit o conexiune, fie către interior, fie către exterior, pentru orice serviciu care folosește porturi cu numere mai mari de 1023. Această breșă poate fi utilizată de hackeri pentru o grămadă de operații, inclusiv pentru comunicația cu un program de tip cal troian.

Pentru a corecta acest set de reguli, trebuie să puteți să specificați, pe lângă portul destinație, și portul sursă. Priviți următorul exemplu:

Rule	Direction	Protocol	Source Address	Dest. Address	Source Port	Dest. Port	Action
1	inbound	TCP	external	internal	>=1024	25	allow
2	outbound	TCP	internal	external	25	>=1024	allow
3	outbound	TCP	internal	external	>=1024	25	allow
4	inbound	TCP	external	internal	25	>=1024	allow
5	*	*	*	*	*	*	disallow

Din acest tabel, puteți observa că regulile 2 și 5 nu mai permit conexiuni între două porturi cu numere mai mari de 1023. În schimb, acele conexiuni trebuie legate, la unul dintre capetele conexiunii, la portul cu numărul 25, caracteristic protocolului SMTP.

Bitul SYN

În figura 5.3, unul dintre câmpurile pe 1 bit este numit SYN. Acest bit de sincronizare este activat atunci când este trimisă o cerere în timpul încercării inițiale de conectare, indicând faptul că numerele de secvență ar trebui sincronizate. Configurarea unei conexiuni consumă mult mai mult timp decât gestionarea uneia care este deja folosită pentru transferul de

date. Informațiile suplimentare solicită numeroase cicluri UCP (de microprocesor) pe măsură ce stratul TCP creează intrări în propriul tabel de stare pentru noua conexiune.

Ce importanță are aceasta când este configurat un firewall? Una dintre metodele uzuale de atac este interzicerea serviciului. O *inundare SYN* nu este decât un hacker care trimite continuu pachete având bitul SYN activat, astfel încât calculatorul destinație pierde mult din timpul prețios al unității centrale de prelucrare încercând să configureze o conexiune nouă și alocând memorie pentru această operație. Cu toate că nu puteți filtra toate pachetele care au activat bitul SYN, puteți monitoriza fișierele jurnal pentru a găsi gazdele care încearcă în mod repetat să trimită aceste tipuri de pachete, astfel încât acelor gazde să nu li se permită accesul prin firewall.

Bitul ACK

Un alt câmp pe 1 bit pe care îl puteți observa în figura 5.3 este ACK, sau bitul de confirmare. Acest câmp este activat numai după stabilirea unei conexiuni. Primul pachet trimis pentru a solicita o conexiune are acest bit șters (dezactivat). La celălalt capăt al conexiunii, acest bit este activat și este trimis înapoi un răspuns. Prin examinarea acestui bit și analizarea direcției comunicației, este posibil să creați reguli în filtrul de pachete pentru a permite o conexiune numai în direcția în care doriți – către interior sau către exterior.

De exemplu, să presupunem că doriți să permiteți clienților dumneavoastră să stabilească o sesiune Telnet de pe stațiile lor de lucru pe un server care se găsește în Internet, însă nu vreți ca aceeași regulă să fie valabilă și în sens invers. Ați putea folosi reguli asemănătoare cu următoarele:

Rule	Direction	Protocol	Source Address	Dest. Address	Source Port	Dest. Port	ACK	Action
1	outbound	TCP	internal	external	>=1024	23	both	allow
2	inbound	TCP	external	internal	23	>=1024	SET	allow
3	*	*	*	*	*	*		disallow

În acest exemplu, puteți vedea că regula 1 permite unei gazde din rețeaua LAN internă să trimită un pachet către un server Telnet din Internet. Aceasta deoarece numărul de port pentru portul destinație este portul 23 de server Telnet, iar dumneavoastră permiteți pachetului să treacă prin filtru indiferent dacă bitul ACK este dezactivat sau activat. Primul pachet pe care gazda internă îl va trimite către portul 23 va avea acest bit șters, în timp ce pachetele următoare îl vor avea activat. Din acest motiv trebuie să permiteți ambele cazuri pentru această regulă de acces în exterior.

A doua regulă permite serverului Telnet din Internet să trimită pachete înapoi către gazda dumneavoastră din interior. Serverul nu va fi capabil să inițieze o sesiune Telnet, deoarece ați indicat în această regulă că bitul ACK trebuie să fie activat, în caz contrar pachetul fiind respins. Deoarece bitul ACK este șters pentru o solicitare inițială de conexiune, această interdicție ar trebui să fie suficientă pentru a împiedica un calculator din exterior să inițieze o sesiune Telnet cu un server din rețeaua LAN internă. Desigur, aceasta dacă aveți un server securizat care să nu aibă instalată pe el o versiune falsificată de server Telnet. Din nou, nu uitați că firewall-ul, în special filtrul de pachete, nu este decât prima linie de

apărare. Trebuie totuși să mențineți și un control atent asupra securității calculatoarelor gazdă din rețeaua dumneavoastră.

Pachete ICMP

Protocolul ICMP (Internet Control Message Protocol) este folosit de stivele TCP/IP pentru a trimite informații de control și gestionare una către cealaltă. De exemplu, un tip de mesaj ICMP este denumit mesaj *Source Quench* (*Oprirea sursei*). Acest tip de mesaj este trimis de un calculator pentru a comunica părții care a inițiat conexiunea să oprească transmisia de pachete. Este folosit pentru controlul fluxului, astfel încât partea receptoare a conexiunii să nu ajungă suprasaturată și să respingă pachetele. Acest tip de mesaj este unul dintre cele pe care nu veți dori să le blocați folosind un filtru de pachete, deoarece gestionarea controlului fluxului este o operație importantă. Mesajul de tip *redirect* poate fi utilizat pentru a comunica unei gazde sau unui ruter că ar trebui folosită o altă rută pentru a ajunge la o anumită destinație. Folosind acest tip de mesaj, un hacker poate trimite date incorecte rutelor dumneavoastră și poate să altereze tabelele de rutare.

Vezi și

- „Protocolul ICMP (Internet Control Message Protocol)”, la pagina 33
- Tabelul 2.1, „Tipuri de mesaje ICMP”, la pagina 34

Pachetele ICMP pot fi foarte utile, însă ele pot fi folosite și pentru a obține informații despre rețeaua dumneavoastră. O funcție importantă a unui firewall este de a împiedica persoanele din exterior să obțină informații despre gazdele din rețeaua dumneavoastră. Datorită acestui fapt, este indicat să blocați câteva tipuri de mesaje, cum ar fi următoarele:

- Mesajele *echo request* către interior și *echo reply* către exterior – Permiteți utilizatorilor dumneavoastră să folosească utilitarul PING pentru a testa conectivitatea cu gazdele din exterior, însă nu și invers.
- Mesajele *redirect* către interior – Aceste mesaje pot fi folosite pentru reconfigurarea tabelor de rutare din rețeaua dumneavoastră.
- Mesajele *destination unreachable* către exterior și *service unavailable* către exterior – Nu permiteți nimănui să vă sondeze rețeaua. Prin aflarea destinațiilor la care nu se poate ajunge sau ce servicii nu sunt oferite, sarcina hackerului este mult ușurată.

Operarea independent de stare în comparație cu inspectarea dependentă de stare

Utilizarea porturilor sursă și destinație pentru crearea regulilor referitoare la conexiunile TCP este foarte utilă. Aceasta se datorează faptului că TCP este un protocol orientat spre conexiune. UDP nu este însă un protocol orientat spre conexiune. Fiecare pachet UDP este independent. Atunci când este folosit pentru a executa funcții de cerere/răspuns, poate fi imposibil de determinat din informațiile de antet ale fiecărui pachet dacă un pachet sosit este un răspuns la un pachet UDP anterior. Un filtru simplu de pachete nu

poate fi utilizat pentru a controla servicii care folosesc pachete UDP de acest gen. Un filtru simplu de pachete, denumit filtru de pachete *independent de stare*, ia decizii în funcție de fiecare pachet în parte și nu puteți crea reguli care să filtreze pachetele pe baza relației între un pachet și altul.

Tehnica de *filtrare dinamică a pachetelor*, denumită și inspectare dependentă de stare, duce conceptul de filtrare a pachetelor la un nivel mai înalt, păstrând în memorie un tabel care încearcă să realizeze corespondența între pachetele către exterior și cele către interior. Informațiile reținute vor fi de obicei adresele sursă și destinație, precum și porturile sursă și destinație. Este folosit un cronometru, astfel că intrările din acest tabel nu pot fi exploatate cu ușurință. Dacă nu apare un răspuns pentru un pachet trimis, intrarea din tabel va fi ștearsă pentru a nu lăsa o breșă în sistemul dumneavoastră de securitate.

Cu toate că un ruter mai vechi nu oferă acest tip de funcționalitate, cele mai multe firewall-uri moderne vă permit să executați acest tip de filtrare.

Filtre de pachete hardware și software

Dacă aveți deja un ruter prin care realizați conectarea rețelei LAN proprii la Internet, probabil dispuneți de capacități de filtrare a pachetelor care ar putea fi folosite ca o primă parte a unui firewall. Dacă vă gândiți că performanța poate deveni o problemă, utilizați un ruter dedicat pentru a efectua filtrarea pachetelor și un alt ruter dedicat pentru a realiza conectarea la Internet. Majoritatea ruterele actuale nu vor avea probleme de performanță, chiar dacă execută ambele funcții. Însă folosirea unui ruter pentru ambele funcții poate face ca operația de configurare a regulilor să fie puțin mai complexă și, astfel, să devină un risc pentru securitate. Dacă există o persoană care răspunde de configurarea rutelui pentru întreținerea tabelelor de rutare, de exemplu, și o altă persoană care răspunde de regulile folosite pentru filtrarea pachetelor, ele ar putea să se încurce reciproc.

Într-o rețea mică, un singur ruter ar trebui să implice un risc mic, deoarece nu aveți decât câteva calculatoare gazdă pe care să le întrețineți și, probabil, mai puține servicii de configurat. Într-o rețea mai mare, este bine să folosiți dispozitive dedicate.

Nu sunteți obligat să folosiți un ruter pentru funcțiile de filtrare a pachetelor ale firewall-ului. Ați putea să utilizați în același scop un calculator gazdă cu două plăci de rețea, având un software configurat corespunzător. Unii furnizori de firewall-uri livrează la un loc filtrele de pachete și serverele intermediare, ca un sistem care să ruleze pe o singură gazdă.

A treia alternativă este un *dispozitiv firewall (firewall appliance)*. Aceste instrumente sunt comercializate ca firewall-uri ușor de instalat, complet funcționale. Unele folosesc ca platformă de bază un sistem de operare UNIX standard, în timp ce altele utilizează o soluție privată. Atunci când analizați aceste tipuri de dispozitive, ar trebui să puneți în balanță ușurința în utilizare, caracteristicile oferite și flexibilitatea interfeței de comenzi și a opțiunilor de înregistrare în jurnal. Mai multe informații despre dispozitivele firewall pot fi găsite în capitolul 20, „Dispozitive firewall”.

Utilizarea unui filtru pentru restricționarea accesului

Ruterele diferă prin sintaxa utilizată pentru crearea listelor de control al accesului (sau a *regulilor*). Unele vă permit să creați un set de reguli care se pot aplica tuturor interfețelor în mod egal, atât către interior, cât și către exterior. Altele vă permit să specificați un set de reguli pentru o interfață și un alt set de reguli pentru cealaltă interfață. Alte produse, cum ar fi CISCO, vă permit să creați seturi de reguli și să le grupați după nume, după care să atribuiți individual unul sau mai multe grupuri la interfețe. Atunci când vă gândiți la cumpărarea unui ruter, ar trebui să vă amintiți că o sintaxă mai flexibilă poate face puțin mai dificilă sarcina de configurare, chiar dacă face ca ruterul să fie mai ușor de adaptat la situații ulterioare, pe măsură ce conexiunile de rețea devin tot mai importante pentru organizația dumneavoastră.

Un alt element care trebuie luat în considerare atunci când alegeți un ruter este metoda folosită pentru introducerea regulilor. De obicei, ruterele au o interfață la care puteți conecta un terminal de tip celulă de caractere sau un PC pentru a stabili o sesiune de comenzi. Cele mai multe rutere vă permit să editați fișiere de configurare pe un alt sistem și să folosiți un program pentru descărcarea fișierului pe ruter. O altă metodă uzuală pentru schimbarea fișierelor de configurare cu un ruter este utilizarea protocolului TFTP (Trivial File Transfer Protocol). De asemenea, păstrarea fișierelor de configurare offline pe un alt sistem face ca recuperarea în urma unei defecțiuni hardware sau a unui alt dezastru să fie un proces mult mai rapid și mai simplu.

Frecvența la care un ruter poate filtra pachete va fi probabil mai mare decât viteza conexiunii la Internet. Ca urmare, pentru majoritatea aplicațiilor nu ar trebui să vă preocupe această problemă.

Între caracteristicile importante ale unui ruter cu filtrarea pachetelor se numără următoarele:

- Capabilități bune de înregistrare în jurnal. De obicei, ruterele au capacitate limitată de stocare, astfel că este recomandată funcția de rutare a informațiilor de tip jurnal la un demon syslogd pe un alt sistem securizat. Ar trebui să fiți capabil să înregistrați atât pachetele refuzate, cât și pe cele cărora li s-a permis trecerea prin firewall.
- O sintaxă de comandă care nu e complicată, permițând crearea regulilor pe baza câmpurilor ce includ portul sursă pentru pachetele TCP și UDP. Folosind această funcție, puteți crea un set de reguli mai sever.
- Regulile ar trebui evaluate în ordine. Dacă ruterul efectuează un anumit tip de „optimizare” a setului de reguli, poate fi dificil să diagnosticați probleme atunci când testați firewall-ul.

Fiți atent atunci când activați protocolul TFTP!

Protocolul TFTP (Trivial File Transfer Protocol) a fost creat pentru scopuri cum ar fi actualizarea unui ruter sau a unui alt dispozitiv de rețea. Acest protocol permite un proces simplu de transfer de fișiere, care nu presupune foarte multe date suplimentare. De asemenea, se descurcă fără un nume de utilizator și o parolă. Din acest motiv, fiți atenți atunci când folosiți TFTP cu un ruter. Asigurați-vă că serviciul este activ numai când îl utilizați, și nu permanent.

Utilizarea unei gazde cu două plăci de rețea pentru restricționarea accesului

O gazdă cu două plăci de rețea poate servi atât ca filtru de pachete, cât și ca server intermediar. Dacă aveți deja un ruter pentru conectarea la Internet, o gazdă cu două plăci de rețea plasată între rețeaua LAN internă, securizată, și ruter poate fi o metodă ieftină pentru crearea unui filtru de pachete. Există practic sute de produse software diferite care pot fi folosite în acest scop. Nu trebuie decât să căutați în Internet folosind textul „firewall” pentru a vedea câte opțiuni există. Multe pot fi chiar descărcate pentru evaluare.

Avantajele și dezavantajele filtrelor de pachete

Filtrul de pachete este primul pas în procesul de creare a unui firewall. Comparate cu serverele intermediare, filtrele de pachete au propriile avantaje și dezavantaje. Câteva dintre avantajele care pot fi obținute prin folosirea unui filtru de pachete sunt următoarele:

- Filtrarea pachetelor este „gratuită”. Dacă aveți deja un ruter, acesta suportă probabil filtrarea de pachete. Într-o rețea LAN mică, un singur ruter poate fi suficient pentru utilizarea ca filtru de pachete.
- Teoretic, nu aveți nevoie decât de un singur filtru, în punctul în care rețeaua LAN proprie se conectează la Internet sau la o rețea externă de calculatoare. Acesta asigură un „punct de strângere” pentru rețea.
- Nu trebuie să instruiți utilizatorii sau să folosiți un tip special de program client sau server pentru implementarea filtrelor de pachete. Ruterul cu ecranare sau gazda pentru filtrarea pachetelor execută în mod transparent toate operațiile pentru clienții din rețeaua dumneavoastră.

În continuare sunt prezentate și câteva dintre cele mai evidente dezavantaje ale filtrelor de pachete:

- Ruterle pot fi dificil de configurat, în special dacă încercați să folosiți o configurație complexă, cu un număr mare de reguli. În această situație, ele pot fi și dificil de testat riguros.
- Atunci când un filtru de pachete se defectează sau nu este configurat corect, pagubele în rețeaua dumneavoastră ar putea fi mult mai mari decât în cazul defectării unui server intermediar. Cu toate că un ruter ar putea permite retransmiterea pachetelor IP datorită unei erori de programare sau unui set de reguli configurat incorect, atunci când o aplicație intermediară se defectează, nu există o retransmisie directă a pachetelor IP. Defectarea unui intermediar desface conexiunea.
- Filtrele de pachete lucrează pe un set mic de date – informațiile din antetul pachetului IP. Deoarece acestea sunt singurele informații care pot fi folosite pentru a decide dacă unui pachet trebuie să i se permită trecerea prin firewall, un filtru de pachete este limitat în ceea ce privește deciziile pe care le poate lua. Tehnicile de inspecție dependente de stare îmbunătățesc această funcție, însă tot ar trebui să luați în considerare folosirea serverelor intermediare (pe lângă un filtru de pachete) pentru a crea o soluție completă de firewall.

- Multe rutere cu filtrarea pachetelor nu au capacități solide de înregistrare în jurnal, astfel că este dificil de obținut informații utile atunci când un sistem este infiltrat sau atacat.

Configurați cu atenție regulile pentru un filtru de pachete, astfel încât să puteți înțelege exact de ce încercați să vă protejați. Testați regulile pentru a vă asigura că funcționează. Folosiți un filtru de pachete la perimetrul rețelei ca o primă componentă a firewall-ului.

Rezumat

Un firewall trebuie să fie format atât dintr-un filtru de pachete, cât și din software intermediar de aplicație. În acest capitol am discutat câteva dintre operațiile pe care le puteți efectua cu un filtru de pachete și despre importanța creării unui set bun de reguli. În următorul capitol, veți analiza o altă componentă importantă a unui firewall: serverul intermediar de aplicație.

Utilizarea unei gazde bastion

- Configurarea unei gazde bastion
- Instalarea unui sistem de operare securizat pornind de la zero
- Eliminarea serviciilor și aplicațiilor care nu sunt necesare
- Ștergerea aplicațiilor și fișierelor care nu sunt necesare
- Protejarea resurselor și controlul accesului
- Configurarea auditării și a înregistrării în jurnal
- Rularea unui software intermediar pe o gazdă bastion
- Compromiterea unei gazde bastion

Configurarea unei gazde bastion

Cele mai multe magazine mari de echipamente de rețea au proceduri de configurare standardizate care sunt utilizate la configurarea serverelor sau a stațiilor de lucru care trebuie plasate în rețea. Capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, a evidențiat importanța stabilirii politicilor care guvernează modul cum trebuie configurate gazdele din rețea. În acest capitol, veți analiza câteva dintre problemele care apar la configurarea unui anumit tip de server în rețeaua dumneavoastră – o gazdă bastion. Acest sistem nu ar trebui să depindă de politicile pe care le stabiliți pentru o stație de lucru sau un server obișnuit din rețea. Configurarea unei gazde bastion presupune luarea în considerare a numeroase aspecte legate de securitate și funcționalitate. Termenul *gazdă bastion* (*bastion host*) este folosit referitor la un sistem de calcul care a fost întărit prin creșterea securității la un nivel care nu este aplicabil pe o stație de lucru obișnuită. Un calculator întărit folosește elementele fundamentale de protecție a resurselor, auditarea și mecanismele de autentificare, din sistemul de operare, în cea mai completă formă. Aplicațiile și serviciile care nu sunt necesare pentru sarcinile efectuate de gazdă bastion sunt eliminate de pe calculator astfel încât să nu poată deveni ținte pentru compromitere. Conturile de utilizator sunt șterse de pe calculator astfel încât să rămână numai cele de care este nevoie pentru rularea software-ului sau cele folosite pentru administrarea gazdei.

Calculatorul „dezbrăcat” este denumit gazdă bastion datorită funcției pe care o îndeplinește. Un firewall bun este compus din mai multe dispozitive. De obicei este utilizat un ruter pentru conectarea rețelei LAN la Internet, iar acest ruter poate fi configurat pentru a efectua operații de filtrare a pachetelor. Filtrul de pachete se găsește în prima linie de apărare între rețeaua LAN și Internet. În spatele acestui filtru de pachete, în funcție de arhitectura pe care ați ales-o pentru firewall, se găsesc de obicei unul sau mai multe calculatoare de tip gazdă bastion care oferă servicii intermediare pentru utilizatorii din rețeaua internă.

O arhitectură cu gazdă ecranată sau cu subrețea ecranată asigură o gazdă sau o subrețea de mai multe gazde care pot fi utilizate pentru a oferi servicii intermediare în spatele unui filtru de pachete. Calculatoarele folosite pentru această funcție sunt gazde bastion. Într-o rețea mică, s-ar putea să fie numai un server care să asigure serviciul de poștă electronică pentru companie și navigarea în Web. Într-o rețea mare, ar putea fi necesară crearea de gazde specializate, fiecare dintre ele rulând un software intermediar pentru o anumită aplicație.

La început efectuați o salvare de siguranță!

În acest capitol, discutăm despre editări ale fișierelor de configurare și eliminarea fișierelor de care nu este nevoie pentru funcționarea gazdei bastion. După ce ați instalat sistemul de operare și sunteți pregătit să începeți procesul de configurare securizată, faceți o salvare de siguranță a sistemului. Dacă împărtășiți problemele de configurare în mai multe procese importante, faceți câte o salvare de siguranță înainte de fiecare proces. Aceasta vă permite să reveniți mult mai repede la o stare anterioară în cazul în care vă dați seama că o operație pe care ați efectuat-o a fost incorectă sau inutilă.

Modul în care configurați gazda bastion nu are legătură cu dimensiunea rețelei. Ar trebui să realizați această operație în cel mai sigur mod posibil, permițând în continuare îndeplinirea sarcinilor atribuite. Securitatea este întotdeauna o balanță între cerințele utilizatorului și amenințările potențiale asupra rețelei. Nu uitați niciodată că zilnic apar în Internet amenințări noi asupra rețelei dumneavoastră. Nu tratați cu ușurință procesul de configurare a unei gazde bastion. Dacă aveți un produs firewall achiziționat din comerț, parcurgeți cu atenție documentația primită de la furnizor. Documentația pentru configurarea produsului ar trebui să menționeze toate problemele de configurare dependente de sistemul de operare pe care trebuie să le aveți în vedere.

Câteva dintre operațiile pe care le veți analiza în acest capitol și care vă pot ajuta să întăriți un calculator pentru a fi folosit ca gazdă bastion sunt următoarele:

- Instalarea unei versiuni securizate a sistemului de operare pornind de la zero.
- Eliminarea serviciilor care nu sunt necesare.
- Eliminarea aplicațiilor pentru utilizatorii finali și a aplicațiilor care nu au legătură cu funcțiile de firewall ale gazdei bastion.
- Folosirea mecanismelor de protejare a resurselor, oferite de sistemele de operare, pentru a controla cu strictețe accesul la toate fișierele și directoarele.
- Configurarea securizată a unei auditări detaliate și a înregistrării în jurnal.

Instalarea unui sistem de operare securizat pornind de la zero

Dacă este posibil, ar trebui să instalați sistemul de operare pentru o gazdă bastion pornind de la zero. Dacă reciclați un sistem mai vechi care are deja instalate un sistem de operare și aplicații, este mai bine să radeți discul și să o luați de la început decât să încercați să analizați și să verificați dacă nu există slăbiciuni. Verificați împreună cu furnizorul dacă aveți ultimele informații despre peticele și actualizările software și nu le aplicați decât pe acelea folosite de suficient timp pentru ca erorile mari de programare și problemele de securitate să fi fost deja descoperite.

Deși nu este practic pentru sistemele de operare, veți vedea că unele sisteme, cum ar fi Open VMS, pot fi încărcate și rulate de pe un CD-ROM. Având sistemul de operare pe CD-ROM sau pe o partiție de disc numai pentru citire, fișierele sistemului de operare nu mai sunt o potențială țintă pentru un intrus. Nu puteți să înlocuiți sau să falsificați fișiere importante de sistem dacă se găsesc pe o partiție numai pentru citire. Unele produse firewall mai răspândite folosesc această tehnică pentru a proteja sistemul de operare și fișierele de aplicații importante. Fișierele care trebuie deschise pentru scriere sau actualizare pot fi stocate pe o altă partiție. Este posibil, pe unele sisteme, ca datele importante să fie plasate complet pe un alt sistem. De exemplu, multe sisteme UNIX pot fi configurate astfel încât demonul syslogd să trimită informațiile de înregistrare în jurnal pe un alt sistem.

De asemenea, este o idee bună să instalați pe gazda bastion numai un sistem de operare. Nu folosiți acest tip de platformă ca gazdă cu încărcare dublă. Orice fișier găsit pe hard-disc este o țintă pe care un hacker o poate folosi împotriva dumneavoastră atunci când a băgat un picior pe ușă. La fel cum eliminați fișierele de aplicații de care nu este nevoie, nu ar trebui să existe ișiere din sistemul de operare pe gazda bastion, cu excepția celor care sunt necesare.

Pentru sistemele UNIX, aveți avantajul unui fișier de parole ascuns dacă această funcție este o componentă a pachetului dumneavoastră de instalare. Această măsură suplimentară de securitate vă ajută să împiedicați un intrus să descarce fișierul obișnuit `/etc/passwd` și să își folosească timpul liber pentru a descoperi parolele dumneavoastră. Dacă fișierul de parole obișnuit este de obicei disponibil pentru toată lumea, fișierul de parole ascuns nu este.

De asemenea, ar trebui să vă gândiți la utilizarea unor metode puternice de autentificare, cum ar fi SecureID sau Skey. Prin utilizarea mecanismelor care asigură parole de unică folosință, securitatea poate fi mult îmbunătățită. Dacă folosiți un dispozitiv fizic extern, cum este o cartelă SecureID care a fost sincronizată cu gazda, gazda bastion devine foarte dificil de depășit.

Pachetele de servicii și corecții pentru Windows NT

Puteți să accesați ultimele pachete de servicii pentru Windows NT vizitând situl www.microsoft.com și folosind butonul de descărcare pentru a localiza pachetele. Atunci când sunt descoperite probleme importante de securitate, ele sunt remediate de obicei cu rapiditate și nu trebuie să așteptați pentru a obține următorul pachet de servicii, care ar putea veni după mai multe luni, pentru a încorpora rezolvarea în sistemul dumneavoastră. Nu trebuie decât să vizitați periodic următorul sit Web pentru a verifica apariția unor corecții noi pe măsură ce sunt furnizate:

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/>

Eliminarea serviciilor și aplicațiilor care nu sunt necesare

Pe sistemele UNIX, procesele care se desfășoară în fundal și oferă servicii sunt denumite *demoni*. Aceste procese demon pot fi proiectate pentru a executa o diversitate de operații, și nu toate sunt necesare pe un calculator pregătit să fie utilizat ca gazdă bastion. De asemenea, serverele Windows NT au procese de tip serviciu care rulează în fundal și pot reprezenta o problemă pe o gazdă bastion. Veți analiza separat cele două cazuri, deoarece sistemele folosesc metode diferite de gestionare a serviciilor rulate în fundal.

UNIX

Pe sistemele UNIX, procesele demon sunt lansate în execuție de obicei prin una din următoarele trei metode:

- De către demonul `inetd`
- De către fișierele de pornire la încărcarea sistemului de operare
- Ca parte a nucleului

Pentru multe servicii uzuale de rețea, demonul `inetd` răspunde solicitărilor apărute în rețea și folosește informațiile din fișierul de configurare propriu, `/etc/inetd.conf`, pentru a lansa în execuție în fundal un proces server care satisface fiecare cerere. Puteți să editați acest fișier pentru a preveni pornirea anumitor servicii nedorite. Dacă această gazdă bastion din firewall este accesată numai de la consola locală, veți dori să eliminați servicii cum ar fi FTP și Telnet, de exemplu.

Vezi și

- Pentru mai multe informații despre fișierul de configurare `inetd.conf`, modul în care este configurat și cum sunt pornite serviciile, vezi secțiunea „Configurarea fișierului `inetd.conf`” din capitolul 13, la pagina 211.

Între serviciile pe care le-ați putea pune în discuție – sau șterge total – din fișierul de configurare `inetd.conf`, se numără următoarele:

- **Serviciile r** – Aceste utilitare convenabile, cum ar fi `rlogin`, `rcp` și `rexec`, sunt convenabile și pentru hackeri. Dacă aceștia sunt capabili să modifice un fișier `hosts.equiv` sau `.rhosts` de pe sistemul țintă, vor fi capabili să provoace pagube mari pe sistemul respectiv. Luați în considerare înlocuirea serviciilor `r`, în cazul în care chiar aveți nevoie de ele, cu serviciile Secure Shell (`ssh`), care execută în esență aceleași funcții, dar adaugă utilităților opțiuni de criptare și autentificare puternică.
- **FTP** – Folosiți un intermediar pentru acest serviciu. Serviciile UNIX standard, cum ar fi FTP și Telnet, trimit parolele sub formă de text clar prin rețea, iar acestea pot fi capturate cu ușurință cu un program de interceptare. Puteți să utilizați pachetul TIS Internet Firewall Toolkit (FWTK), de exemplu, pentru a oferi un serviciu FTP mai sigur către și dinspre firewall.

Vezi și

Pentru mai multe informații despre FWTK, vezi capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)”, la pagina 217.

- **Telnet** – Ca și în cazul FTP, folosiți un intermediar, cum ar fi, de exemplu, unul dintre cele disponibile în pachetul FWTK.
- **uucp** – Cu toate că nu este la fel de răspândit ca altădată, programul uucp (UNIX to UNIX Copy Program) este încă inclus în unele versiuni UNIX și mai poate fi găsit rulând în unele locuri. Acest utilitar a fost scris în perioada de început a rețelei Internet și a protocoalelor TCP/IP și nu este o metodă sigură de distribuire a informațiilor între calculatoare în rețeaua Internet modernă. Funcționalitatea oferită de uucp a fost înlocuită de alte utilitare care sunt mai ușor de utilizat și care operează într-un mod mai securizat.
- **finger** – Acest utilitar UNIX standard vă oferă informații despre utilizatorii din rețea. Amintiți-vă că doriți să faceți disponibile cât mai puține informații posibile de pe gazda firewall. Dacă doriți neapărat să folosiți utilitarul finger, luați în considerare înlocuirea fișierului executabil standard cu unul dintre utilitarele finger „sigure” existente în Internet.

Vezi și

➤ Vezi anexa B, „Alte instrumente de securitate pe care le puteți folosi”, la pagina 364.

- **inetd** – Este posibil să ștergeți chiar serverul demon inetd, deoarece multe produse comerciale oferă această funcționalitate. Pentru a găsi înlocuitori pentru serviciile r, verificați produsul SSH Secure Shell, care poate fi folosit în locul acestor servicii problematice.

Dacă aveți nevoie să utilizați unul dintre serviciile de rețea standard, cum ar fi Telnet sau FTP, pentru a accesa gazda bastion de la distanță, puteți să folosiți pe acest calculator produsul TCP Wrappers sau un alt produs echivalent. TCP Wrappers vă permite să creați o sesiune Telnet relativ sigură cu gazda bastion pentru gestionarea resurselor folosind o poartă Telnet. Produsul TCP Wrappers poate fi configurat pentru a utiliza tehnici puternice de autentificare și pentru a înregistra toate încercările reușite sau eșuate prin syslogd.

Vezi și

➤ Pentru mai multe informații despre TCP Wrappers și modul său de configurare, vezi capitolul 13, „Utilizarea produsului TCP Wrappers”, la pagina 208.

Ce este Secure Shell?

Secure Shell este un set de utilitare care folosesc protocolul SSH și care permit servicii similare cu serviciile r de la Berkeley pentru a lucra într-un mod care nu prezintă riscuri evidente de securitate. Pentru a face utilitarele sigure, sunt utilizate tehnici de criptare punct-la-punct și tehnici puternice de autentificare. Cea mai nouă versiune a protocolului este SSH2, care include suport pentru protocolul SFTP (Secure File Transfer Protocol) și pentru mai mulți algoritmi cu chei publice. Pentru a afla mai multe informații despre Secure Shell, puteți vizita adresele URL www.ssh.org sau www.ssh.com/products/ssh/.

Priviți conținutul fișierului inetd.conf pentru a localiza și alte servicii triviale sau servicii în care nu aveți încredere. De exemplu, dacă folosiți un demon talkd pentru a permite utilizatorilor să se angajeze în conversații folosind tastatura, acest serviciu este dificil de justificat pe o gazdă bastion. Unele situri utilizează una sau mai multe copii „standar-

dizate” ale unui fișier inetd.conf creat ca o măsură politică pentru a avea siguranța că există copii identice pe anumite tipuri de sisteme, cum ar fi stații de lucru sau servere. Dacă aceasta este și situația din situl dumneavoastră, respingeți fișierul și luați-o de la început, listând doar serviciile care trebuie neapărat să ruleze pentru ca gazda bastion să execute propriile funcții de firewall. Serviciile convenabile sau distractive ar trebui să fie mutate pe alte sisteme care se găsesc într-un mediu mai protejat. Gazda bastion este activă pe linia frontului apărării dumneavoastră și nu trebuie utilizată pentru nimic altceva.

Unele servicii sunt pornite la încărcarea sistemului, în general din fișierele /etc/rc.*. Verificați în documentație pentru a găsi structura corespunzătoare a directorului cu fișierele de pornire și pentru a determina ce fișiere sunt pornite simultan cu procesele. Acesta este modul obișnuit în care sunt pornite servicii cum ar fi NFS (Network File System). NFS este un sistem complex, construit pe baza unor rutine care folosesc apeluri de proceduri de la distanță (RPC, sau remote procedure call). Protocolul Mount este utilizat pentru a realiza conexiunea inițială cu sistemul de fișiere situat la distanță.

RPC este o aplicație protocol simplă de tip client/server care definește modul în care interacționează clienții și serverele. A fost dezvoltată inițial pentru a fi utilizată în construirea sistemului NFS, însă în prezent este folosită pe scară largă pentru multe alte servicii. Atât clienții, cât și gazdele server care folosesc RPC rulează demonul rpcbind.

NFS este un protocol independent de stare. Aceasta înseamnă că serverul nu păstrează informații care să țină evidența de la o cerere a unui client la următoarea. NFS nici nu lucrează cu funcții de genul deschidere sau închidere de fișier, care v-ați putea aștepta să fie necesare într-un sistem de fișiere distribuit în rețea. Există un alt protocol, Mount, care execută această funcție pentru NFS. Aceasta înseamnă că un alt serviciu în fundal, demonul mountd, rulează atât pe client, cât și pe calculatorul server.

De ce nu ar trebui să utilizați NFS pe un server situat aproape de Internet?

NFS este un sistem de fișiere distribuit în rețea. Deși ar putea fi foarte convenabil de folosit în rețeaua locală pentru a permite mai multor utilizatori să partajeze fișiere în rețea, doriți să faceți aceste fișiere și directoare disponibile pentru montare unei persoane din afara rețelei dumneavoastră – unei persoane din Internet? Măsurile de securitate pe care le veți găsi în diferite implementări ale sistemului NFS nu sunt suficiente pentru a permite acest tip de serviciu pe legături în care nu aveți încredere.

După cum puteți observa din această scurtă discuție, dacă rulați NFS pe o gazdă, în realitate rulați mai multe procese în fundal. Probabil că cel mai problematic dintre ele este demonul RPC, deoarece foarte multe servicii au fost implementate folosind acest demon. Problema este că ar trebui să analizați cu atenție fișierele de pornire pentru sistemul UNIX (sau Linux) propriu și să eliminați orice serviciu care nu este absolut necesar! Instalările prestabilite executate de programele de configurare pot lăsa în urmă o mulțime de lucruri despre care nu aveți cunoștință. Hackerii știu să caute astfel de lucruri și să găsească metode prin care să le activeze sau să abuzeze de aceste fișiere uitate. Verificați documentația versiunii UNIX (sau Linux) pe care o aveți și aflați ce componente ale nucleului pot fi eliminate fără probleme. Recompilați nucleul (și nu lăsați vechea versiune în calculator) și testați dacă modificările efectuate funcționează așa cum trebuie.

Mai multe informații despre NFS

De când Sun Microsystems a dezvoltat pentru prima dată protocoalele Network File Systems, tehnologia a fost îmbunătățită și portată pe multe variante de UNIX și pe alte sisteme de operare. Pentru a învăța mai multe despre

modul de lucru al protocoalelor NFS, citiți documentul RFC 1094, care definește cea mai utilizată versiune de NFS (versiunea 2). Documentul RFC 1813 prezintă versiunea 3, care adaugă un suport mai bun pentru lucrul în rețele de mare suprafață.

Alte fișiere UNIX de rețea care trebuie revizuite

După ce terminați editarea fișierelor utilizate pentru configurarea sau pornirea serviciilor de rețea, mai există și alte fișiere pe care ar trebui să le analizați. Dacă încă folosiți fișierul `/etc/hosts`, indiferent de motivul pentru care o faceți, verificați dacă nu este o copie a unui fișier de pe un alt sistem cu informații despre gazda respectivă, care nu sunt necesare pe serverul gazdă bastion. Dacă gazda bastion este compromisă, orice informație pe care o poate găsi un hacker și care descrie rețeaua dumneavoastră sau gazdele din această rețea poate să servească pentru a face mai ușoare și alte intruziuni în rețea.

Printre alte fișiere de configurare de rețea standard în sistemele UNIX, care trebuie verificate, se numără următoarele:

- `/etc/networks` Acest fișier este similar cu fișierul `/etc/hosts`, care mapează numele prietenoase la adresele IP. Acest fișier face același lucru pentru adresele de rețea. Deși este convenabil să referiți gazdele de la distanță după nume, pentru mulți utilizatori finali această funcționalitate (a numelui de rețea) nici nu este necesară. Majoritatea utilizatorilor finali nu au nici o idee despre rețelele la care sunt conectați. Acest fișier nu este folosit decât pentru a defini numele rețelei locale pentru traducerea adresei, însă ar trebui analizat pentru a vă asigura că nu conține înregistrări care nu sunt necesare sau care arată ciudat.
- `/etc/protocols` Acest fișier este folosit pentru a asocia un număr cu un nume de protocol. De exemplu, antetul pachetului IP conține un câmp care definește dacă pachetul este pentru protocolul TCP sau pentru protocolul UDP. În pachetul IP, protocolul este identificat după un număr. Acest număr poate fi referit încrucișat în fișierul `/etc/protocols` pentru a obține numele protocolului. Verificați dacă o instalare de aplicație sau o altă procedură de configurare nu a adăugat protocoale noi, pe care nu le utilizați, în acest fișier.
- `/etc/services` Acest fișier realizează corespondența între numele serviciului de rețea și numărul de port utilizat în mod obișnuit de serviciu și de protocolul de transport (TCP sau UDP) folosit de serviciu. Puteți să editați din proprie inițiativă acest fișier dacă doriți să adăugați mai mult de un tip de server pentru un software intermediar particular. De exemplu, ați putea să creați două versiuni ale demonului Telnet utilizând pachetul TIS Internet Firewall Toolkit, fiecare demon folosind un număr de port diferit.

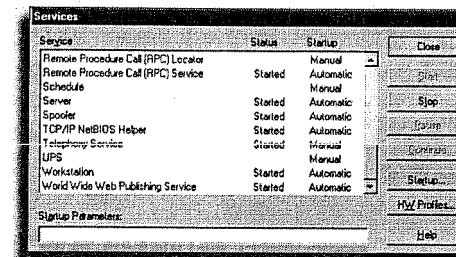
Ce servicii rulează?

Pentru a vedea ce servicii rulează curent pe sistem, folosiți comanda `ps`. Această comandă vă oferă o rapidă trecere în revistă a proceselor rulate pe sistem. Răspunsul dat depinde de varianta de sistem UNIX, dar constă în general din câte o linie pentru fiecare proces, în care este afișată comanda care este executată, împreună cu alte informații, cum ar fi identificatorul de proces (PID) și identificatorul UID sub care rulează. După ce ați eliminat serviciile care nu sunt necesare de pe un sistem, reporniți-l și folosiți această comandă pentru a verifica ce procese ați uitat în fișierele de pornire sau în configurarea nucleului. Utilizați această comandă atunci când monitorizați sistemul pentru a vă asigura că demonul `inetd` nu pornește servicii neautorizate.

Windows NT

FIGURA 6.1

Miniaplicația Services vă permite să gestionați serviciile care rulează pe un sistem Windows NT Server.

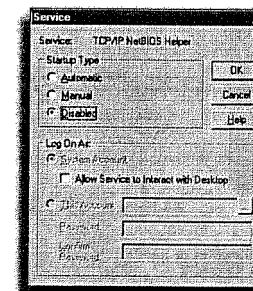


serviciile într-o zonă derulabilă. Puteți să derulați în sus și în jos pentru a localiza toate serviciile configurate curent pe sistem.

Folosind acest utilitar, puteți să porniți, să opriți sau să întrerupeți temporar serviciile. Deși este recomandată oprirea unui serviciu, este o idee bună și ștergerea completă din sistem a unui serviciu în cazul în care acesta nu este necesar. De exemplu, în figura 6.1 serviciul TCP/IP NetBIOS Helper rulează. Deoarece serverul nu folosește decât protocolul TCP/IP pentru comunicarea cu clienții sau cu alte sisteme din Internet, nici nu trebuie să aveți instalat protocolul NetBIOS. Faceți o listă cu serviciile afișate de acest utilitar, dezactivați-le și apoi începeți să le ștergeți.

FIGURA 6.2

Folosind această casetă de dialog, stabiliți ca un serviciu să fie dezactivat la pornire.



Pentru a dezactiva un serviciu de rețea, inițial trebuie să îl opriți executând clic pe serviciu și utilizând butonul Stop. Apoi folosiți butonul Startup pentru a schimba modul în care este pornit serviciul. În figura 6.2 puteți vedea caseta de dialog Service.

Pentru a șterge un protocol sau serviciu de rețea din sistem, utilizați miniaplicația Network din Control Panel. În figura 6.3, puteți vedea miniaplicația Network având selectată pagina

Services. Dacă protocolul NetBIOS nu este folosit de sistem, puteți să ștergeți aici acest serviciu în această casetă executând clic pe el și apoi executând clic pe butonul Remove. Pentru a duce lucrurile puțin mai departe, puteți să ștergeți și protocolul NetBEUI. Figura 6.4 prezintă miniaplicația Network având selectată pagina Protocols. Aici, puteți să executați clic pe protocolul NetBEUI și apoi să folosiți butonul Remove pentru a șterge protocolul de pe server.

Înainte de a începe eliminarea serviciilor sau protocoalelor, verificați documentația pentru a găsi aplicațiile intermediar sau software-urile firewall care vor rula pe server. S-ar putea să găsiți sugestii specifice referitoare la protocoalele și serviciile care trebuie șterse, ca și la modul de configurare a celor care vor rămâne pe sistem.

FIGURA 6.3

Pentru a șterge un serviciu, selectați-l și executați clic pe butonul Remove.

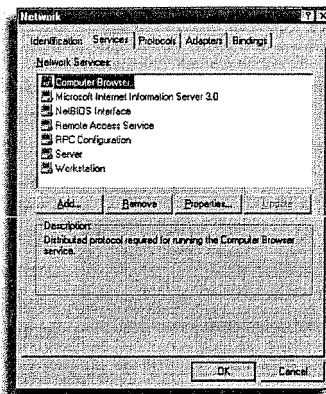
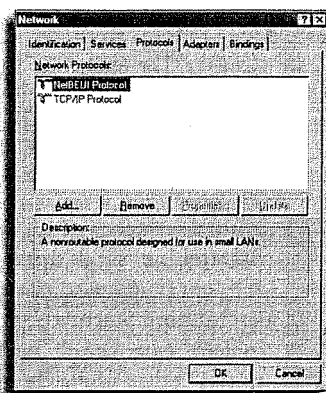


FIGURA 6.4

Folosiți pagina Protocols pentru a șterge protocoalele de rețea de pe server.



Ștergerea aplicațiilor și fișierelor care nu sunt necesare

După ce ați șters serviciile care nu mai sunt necesare pe gazda bastion, faceți curățenie și ștergeți și programele executabile pe care le folosesc aceste servicii. Orice lăsați în urmă și ajunge sub ochii unui intrus ar putea fi util pentru compromiterea ulterioară a sistemului.

Atunci când un calculator este „curățat” pentru a fi transformat într-o gazdă bastion, ar trebui lăsat pe el numai software-ul necesar. Pe lângă ștergerea conturilor de utilizator și a serviciilor care nu mai sunt necesare, nu uitați să verificați alte aplicații la care poate avea acces gazda respectivă. De exemplu, pe o gazdă bastion nu este nevoie probabil de nici un fel de compilator. De ce ați avea nevoie să compilați un program pe un astfel de sistem? Nu puteți să executați operația de compilare pe un alt sistem, poate chiar pe unul dedicat? Din sistemul de fișiere al unei gazde bastion ar trebui șterse și alte instrumente de dezvoltare, incluzând aici fișierele bibliotecă și de scripturi.

O gazdă bastion ar trebui să se concentreze numai pe funcțiile pe care le execută pentru firewall. Nu aveți nevoie de o aplicație de prelucrat texte sau de un program de calcul tabelar din ultima generație pe gazda bastion, deoarece nu ar trebui să efectuați astfel de activități pe acest tip de mașină. Dacă ați executat o instalare curată a sistemului de operare, verificați documentația (și sistemul care rulează) pentru a determina dacă, în mod prestabilit, ați instalat și alte aplicații care nu sunt necesare.

De exemplu, o instalare standard a sistemului Windows NT este foarte încărcată cu accesorii care se justifică foarte rar pe o gazdă bastion firewall. Folosiți miniaplicația Add/Remove Programs din Control Panel pentru a șterge aplicațiile de care nu este nevoie, cum ar fi jocurile, Microsoft Photo Editor, Calculator și așa mai departe. Veți păstra WordPad sau NotePad pentru a le folosi la editarea fișierelor din sistem, însă majoritatea celorlalte accesorii pot fi eliminate.

Chiar dacă aveți nevoie pe calculatorul gazdă de un editor pentru executarea operațiilor de gestionare, nu vă trebuie mai multe editoare. UNIX are mai multe editoare foarte populare și de obicei găsiți mai multe editoare în orice versiune comercială a acestui sistem de operare. Faceți sarcina hackerului mai dificilă reducându-i variantele de alegere. Stabiliți ce editor este cel mai simplu de utilizat pentru dumneavoastră și ștergeți-le pe celelalte.

Atunci când trebuie să testați un produs sau o componentă nouă pentru un firewall, încercați să efectuați această operație într-un laborator înainte de a instala produsul pe o gazdă bastion. După ce ați instalat software-ul pe o gazdă bastion, asigurați-vă că îl ștergeți atunci când nu mai aveți nevoie de el. Poate fi tentant să lăsați instalate pe sistem utilitare demon sau alte produse de test peste data lor de expirare. Deși aplicația poate părea că nu pune nici o problemă, nu ar trebui să lăsați în urmă lucruri pe care un hacker va ști cum să le exploateze, fie că este vorba de un software executabil, fie ceva de genul unei structuri de directoare creată de aplicație.

Protejarea resurselor și controlul accesului

Pentru a securiza sistemul de operare, ca și aplicațiile care vor rula pe gazda bastion, familiarizați-vă cu tehnicile permisiunilor de resurse întrebuințate de sistemul de operare. UNIX și Windows NT folosesc termeni similari pentru a descrie controlul accesului, cum ar fi termenii standard read (citire), write (scriere) și execute (execuție). Semnificația lor și modul în care pot fi gestionate sunt mult diferite între cele două sisteme de operare. Windows NT utilizează un mediu grafic GUI în care indicați și executați clic, în timp ce UNIX folosește o interfață în linie de comandă.

Permisuniile la resurse UNIX

Sistemul de operare UNIX vă permite să atribuiți permisiuni la fișiere și directoare pe baza a trei categorii fundamentale. Primul grup de permisiuni se aplică proprietarului fișierului sau directorului. Al doilea se aplică grupului de utilizatori cărui îi aparține fișierul. Al treilea specifică permisiunile pentru alți utilizatori care încearcă să obțină acces la fișier. Tipurile de permisiuni fundamentale pe care le puteți aplica unui fișier sau director sunt următoarele:

- **Read (r)** Această permisiune acordă utilizatorului dreptul să listeze fișierele stocate într-un director (inclusiv atributele acestuia) și permite citirea conținutului unui fișier.
- **Write (w)** Această permisiune acordă utilizatorului dreptul să adauge sau să șteargă fișiere într-un director și să modifice conținutul unui fișier.
- **Execute (x)** Această permisiune acordă unui utilizator dreptul de a accesa directorul și de a lansa în execuție un fișier program.

Vizualizarea valorilor permisiunilor

Pentru a vedea ce valori de permisiuni sunt atribuite unui fișier sau director, puteți utiliza comanda `ls`, ca în exemplul următor:

```
ls -l /usr/bin/fwadm
dr-xr-xr-x 1 fwadm bca 0 Jan 1 2000 html
dr-xr-xr-x 1 fwadm bca 0 Feb 3 2000 documents
-r-xr-xr-x 1 fwadm bca 1624 Feb 6 2000 sources.txt
-r-xr-xr-x 1 fwadm bca 1624 Feb 22 2000 misc.dat
```

Primul șir de caractere, denumit *tablou de permisiuni*, din fiecare linie a listingului este folosit pentru a determina tipul de intrare (director sau fișier) și permisiunile asociate cu intrarea. Primele două linii din acest listing prezintă fișiere de tip director, indicate de caracterul `d` cu care începe acest șir pentru intrările amintite. Următoarele două intrări sunt fișiere obișnuite, indicate de caracterul cratimă (`-`) cu care începe șirul. S-ar părea că cele trei câmpuri rămase pot fi determinate după cratimele rămase în șir. Însă nu este adevărat. Fiecare poziție din șir care urmează bitului de director poate fi o permisiune acordată sau interzisă. Caracterul cratimă este folosit pentru a arăta că permisiunea respectivă nu este acordată.

De exemplu, pentru directorul `html`, tabloul de permisiuni este `dr-xr-xr-x`. Acest șir poate fi separat în patru părți:

- **Poziția 1** Indică directorul sau fișierul.
- **Pozițiile 2-4** Valorile permisiunilor pentru proprietar (Owner).
- **Pozițiile 5-7** Valorile permisiunilor pentru grup (Group).
- **Pozițiile 8-10** Valorile permisiunilor pentru toți ceilalți utilizatori (All others).

Ca urmare, tabloul de permisiuni este un șir de 10 caractere și toate pozițiile sunt semnificative. În exemplul cu directorul `html`, permisiunile pot fi interpretate în felul următor:

- **Proprietar** Permisiune pentru citire și execuție
- **Grup** Permisiune pentru citire și execuție
- **Toți ceilalți** Permisiune pentru citire și execuție

Cu aceste valori de configurare, nimeni nu are acces pentru scriere în acest director.

SUID și SGID

Pe lângă aceste permisiuni de bază, mai există două permisiuni importante care trebuie discutate: SUID și SGID. Atunci când un program rulează pe un sistem UNIX, folosește permisiunile care se aplică utilizatorului care rulează programul. Dacă utilizatorul este

proprietarul fișierului, sunt folosite permisiunile proprietarului. Dacă utilizatorul este membru al aceluiași grup ca și programul, se aplică permisiunile grupului.

Însă dacă unui program îi este aplicată permisiunea SUID (Set User ID), atunci când este executat preia un set de permisiuni identice cu cele ale proprietarului fișierului, chiar dacă utilizatorul care rulează programul nu este proprietarul acestuia. În mod similar, permisiunea SGID (Set Group ID) permite programului să obțină permisiunile care vor fi acordate grupului. Aceste permisiuni puternice permit rularea unui program pentru a executa funcții care ar trebui să fie interzise utilizatorului dacă acesta ar încerca să le execute direct. Este o facilitare necesară pentru anumite proceduri. De exemplu, atunci când un utilizator își schimbă parola, aplicația pentru parolă accesează fișierul `/etc/passwd` având accesul pentru scriere în vederea efectuării modificării. Utilizatorul nu are acces pentru scriere în fișierul `/etc/passwd`, astfel că aplicația pentru parolă trebuie să fie capabilă să obțină singură permisiunea. Problema cu aceste permisiuni nu provine de la utilizarea lor normală, ci din erori de programare sau obiceiuri greșite de programare.

Atunci când un program utilizează aceste permisiuni și există o eroare de programare cunoscută, este posibil ca un hacker să exploateze această eroare pentru a sparge cadrul programului și apoi, având permisiuni superioare, să execute funcții pe care dumneavoastră nu intenționați să le efectuați. Un obicei bun de programare este verificarea stărilor de răspuns ale tuturor rutinelor și detectarea tuturor erorilor care pot fi determinate prin această metodă.

Pentru a determina dacă un fișier sau un director a avut activată permisiunea SUID, puteți să folosiți tot comanda `ls` și să căutați litera `S` în câmpul de permisiune al proprietarului din tabloul de permisiuni. Aceasta indică permisiunea SUID. Dacă această literă este majusculă, permisiunea de execuție nu este acordată pentru proprietar. Dacă litera este mică, proprietarului îi este acordată permisiunea de execuție.

Atunci când permisiunea este stabilită pentru un grup (adică este acordată permisiunea SGID), veți găsi caracterul `s` în poziția utilizată pentru accesul la execuție al grupului.

Schimbarea proprietarului și a valorilor permisiunilor

Există două comenzi simple pe care le puteți folosi pentru schimbarea proprietarului și a permisiunilor la resurse. Acestea sunt `chown` (change owner) și `chmod` (change permission mode). Pentru a schimba proprietarul unui fișier sau director, folosiți următoarea sintaxă:

```
chown [ -fhr ] owner [: group ] file...
```

În această sintaxă, *owner* (sau *group*) ar trebui să fie noul utilizator sau identificatorul grupului căruia doriți să îi acordați proprietatea asupra fișierului sau directorului (*file...*). Parametrii pe care îi puteți folosi vor acționa astfel:

- **-f** Anulează raportarea erorilor.
- **-h** Schimbă proprietarul pentru o legătură simbolică la un fișier și nu pentru fișierul real.
- **-R** Determină ca schimbarea proprietarului să fie aplicată și pentru fișierele și directoarele din directorul curent.

Pentru a schimba permisiunile de acces la un fișier sau director, folosiți comanda `chmod`. Sintaxa pentru această comandă vă permite să folosiți două metode diferite pentru specificarea permisiunilor. Prima utilizează o valoare numerică, în timp ce a doua metodă

folosește un șir de text. Pentru a fi puțin mai clar, haideți să analizăm la început valorile numerice pe care le puteți folosi pentru a specifica permisiunile:

- 0 No access (Nici un acces)
- 1 Execuție fișier (sau căutare în director)
- 2 Write (Scriere)
- 4 Read (Citire)

Pentru a schimba permisiunile de acces la un fișier folosind aceste valori, specificați câte o cifră pentru fiecare câmp (proprietar, grup și ceilalți utilizatori). Pentru fiecare dintre acestea, puteți să adunați valorile pentru mai multe permisiuni și să ajungeți astfel la o valoare între 0 și 7.

De exemplu:

```
chmod 660 /etc/bca/sw2dd.asc
```

În acest caz, au fost stabilite permisiunile de citire și scriere (4+2=6) pentru proprietar și grup. Pentru toți ceilalți utilizatori este interzis accesul la fișier (0).

A doua metodă pe care o puteți folosi pentru a schimba valorile permisiunilor pentru un fișier sau director utilizează caractere în loc de valori numerice.

Pentru a specifica pentru cine este stabilită valoarea de permisiune, sunt folosite următoarele litere:

- u Owner (Proprietar)
- g Group (Grup)
- o Others (Ceilalți)
- a All (Toți)

Pentru a specifica permisiunea acordată, folosiți următoarele caractere:

- r Read (Citire)
- w Write (Scriere)
- x Execute (Execuție)
- s SUID sau SGID

Pentru a utiliza comanda `chmod`, trebuie să specificați cui i se aplică schimbarea de permisiune, ce permisiune este adăugată sau anulată și fișierul sau directorul pentru care este stabilită modificarea. Sintaxa pentru această operație este următoarea:

```
chmod who function permission
```

Pentru *who* și *permission* folosiți caracterele pe care tocmai le-ați văzut. Pentru *function*, puteți utiliza oricare dintre următoarele variante:

- = Pentru a stabili o permisiune
- + Pentru a adăuga o permisiune
- - Pentru a șterge o permisiune

De exemplu:

```
chmod a=rw /etc/bca/sw2dd.asc
```

Această comandă oferă tuturor (a provine de la *all*) permisiunile de citire (r) și scriere (w) în fișier. În exemplul următor, anulăm accesul de scriere (w) pentru celelalte grupuri:

```
chmod o-w /etc/bca/sw2dd.asc
```

Windows NT

Atunci când instalați sistemul Windows NT (sau Windows 2000) pe o partiție formatată folosind sistemul NTFS, permiteți capabilitatea de configurare a protecțiilor la resurse până la nivelul de fișier unic. Aceasta se aplică pe fiecare disc al sistemului formatat folosind sistemul NTFS, și nu numai pe partiția pe care instalați sistemul de operare Windows NT. Folosirea unei partiții FAT, care nu permite configurarea protecțiilor la resurse pentru fișiere sau directoare individuale cu un sistem de operare Windows, nu este acceptabilă pe un calculator gazdă care rulează Windows NT și operează ca parte a unui firewall.

Pentru a începe analiza tipurilor de permisiuni care pot fi utilizate pentru a controla resursele pe o platformă Windows NT, trebuie să analizați inițial cele două metode folosite. Puteți utiliza *permisiunile speciale*, care sunt de bază, sau să atribuiți permisiuni folosind grupuri care combină câteva dintre aceste permisiuni de bază într-o unitate în vederea atribuirii.

Permisiunile speciale vă oferă cel mai complet control asupra accesului la resurse:

- R Permisiunea Read (Citire)
- W Permisiunea Write (Scriere)
- X Permisiunea Execute (Execuție)
- D Permisiunea Delete (Ștergere)
- P Permisiunea Change (Modificare)
- O Permisiunea Take Ownership (Luare în proprietate)

Majoritatea permisiunilor standard care pot fi folosite pentru fișiere combină câteva dintre aceste permisiuni speciale (care sunt mult mai precise) în unități care pot fi mai convenabil de utilizat la atribuirea permisiunilor:

- Read RX
- Change RWXD
- Full Control RWXDPO
- No Access

Dacă priviți permisiunea standard Read, puteți observa că include permisiunea specială Read, ca și permisiunea specială Execute. Atunci când acordați unui utilizator dreptul de a citi un fișier, în majoritatea cazurilor doriți ca utilizatorul respectiv să fie capabil să execute fișierul. Într-o astfel de situație, utilizarea permisiunii Read este mai simplă decât utilizarea permisiunilor speciale și efectuarea de două atribuiri de permisiuni, una pentru accesul la citire și alta pentru accesul la execuție. O permisiune standard pe care o puteți folosi și care nu este formată din mai multe permisiuni speciale este No Access. Această permisiune este o metodă convenabilă de interzicere a oricărui tip de acces la o resursă.

Pentru directoare, există o listă diferită de permisiuni standard. Atunci când definiți acest tip de permisiuni, există două seturi de permisiuni listate: cele care se aplică directorului și cele care se aplică fișierelor din director. Permisiunile standard pentru directoare sunt următoarele:

- List (RX) (nespecificat)
- Read (RX) (RX)
- Add (WX) (nespecificat)
- Add & Read (RWX) (RX)
- Change (RWXD) (RWXD)

- Full Control (RWXDPO) (RWXDPO)
- No Access

În această listă puteți observa că permisiunea Read operează pentru directoare la fel cum operează pentru fișiere; sunt acordate atât accesul pentru citire, cât și accesul pentru execuție în director. În plus, și fișierelor create în director le sunt acordate permisiunile de citire și execuție. Fișierele create într-un director moștenesc permisiunile de la director. Rețineți că nu toate permisiunile standard pentru directoare operează pentru a acorda acelea permisiuni directorului și respectiv fișierelor acestuia. De exemplu, dreptul Add & Read acordă accesul la citirea, scrierea și execuția fișierului din director. Însă fișierele create în director nu moștenesc decât drepturile de citire și execuție.

Vizualizarea proprietarului și a permisiunilor pentru fișiere și directoare

Pentru a vizualiza permisiunile oricărui fișier sau director, puteți utiliza programul Windows Explorer.

Vizualizarea permisiunilor cu Windows Explorer

1. Executați clic pe Start, Programs, Windows NT Explorer. În figura 6.5, puteți vedea că a fost selectat dosarul IIS fw.

FIGURA 6.5

Programul Windows NT Explorer poate fi utilizat pentru a vizualiza fișierele și directoarele și pentru a gestiona permisiunile.

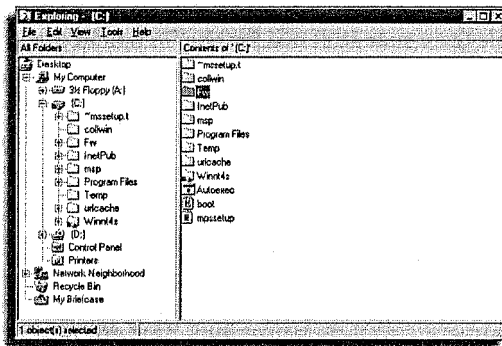
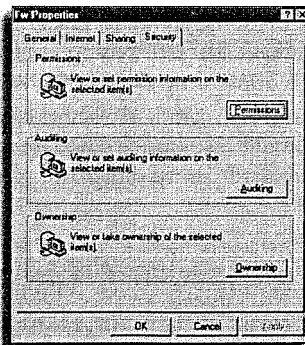


FIGURA 6.6

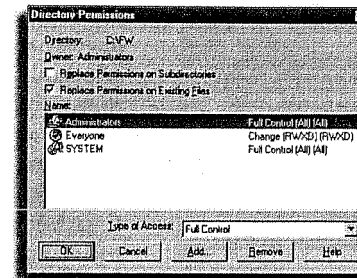
Foia Security Properties (Proprietăți de securitate) pentru dosar poate fi folosită pentru modificarea permisiunilor.



2. Executați clic cu butonul drept al mouse-ului pe un dosar sau fișier și selectați din meniu opțiunea Properties. În figura 6.6, puteți vedea pagina Properties pentru dosarul fw, având selectată foaia de proprietăți Security.
3. Executați clic pe butonul Permissions pentru a modifica permisiunile de resurse ale dosarului.

FIGURA 6.7

Caseta de dialog Directory Permissions poate fi utilizată pentru a afișa permisiunile existente.



4. Utilizați caseta de dialog Directory Permissions (Permisuni pentru director) care apare pe ecran (figura 6.7) pentru a vizualiza permisiunile existente pentru dosar. În mod curent, există mai multe grupuri de utilizatori care au acordate permisiuni de acces pentru acest dosar.

Modificarea permisiunilor

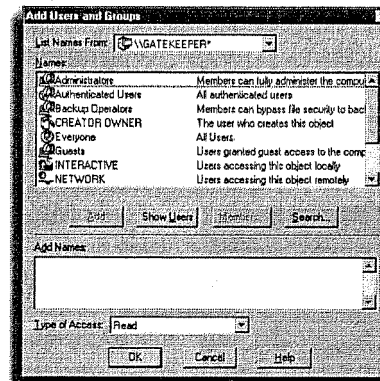
În exemplul anterior, există un dosar în care atât grupul Administrators, cât și contul System au acces cu control complet asupra directorului. Grupul Everyone are permisiunea Change. Să presupunem că tocmai ați creat un cont nou de utilizator, denumit fwadmin1, și doriți să îi acordați acces cu control complet să îl ștergeți din grupurile Administrators și Everyone. Puteți să efectuați modificările folosind programul Windows NT Explorer. La început, localizați dosarul sau fișierul pe care doriți să îl modificați utilizând aplicația Explorer și deschideți caseta de dialog Directory Permissions, așa cum ați procedat în exemplul anterior.

Modificarea permisiunilor cu Windows Explorer

1. În caseta de dialog Directory Permissions, bifați casetele de validare Replace Permissions on Subdirectories (Înlocuiește permisiunile asupra subdirectoarelor) și Replace Permissions on Existing Files (Înlocuiește permisiunile asupra fișierelor existente).

FIGURA 6.8

Caseta de dialog Add Users and Groups vă permite să selectați utilizatorii cărora li se va acorda acces.

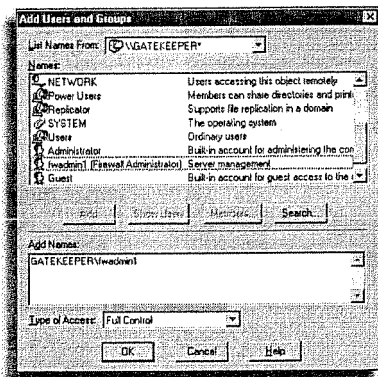


fwadmin1 (vezi figura 6.9). Executați clic pe butonul Add și contul GATEKEEPER\fwadmin1 este afișat în câmpul Add Names (Adaugă nume).

4. Executați clic pe butonul OK pentru a reveni în caseta de dialog Directory Permissions. Contul de utilizator fwadmin1 este acum afișat prezentând permisiunea de acces Full Control.

FIGURA 6.9

Selectați tipul de acces și un cont de utilizator (sau grupul de utilizatori).



5. Reveniți din nou în caseta de dialog Directory Permissions, selectați grupul Administrators executând clic pe el și apoi executați clic pe opțiunea Remove. Procedați în mod similar pentru grupul Everyone. Caseta de dialog Directory Permissions ne arată acum că numai utilizatorului fwadmin1 și contului special SYSTEM le este permis accesul la acest dosar. Deoarece au fost selectate ca-

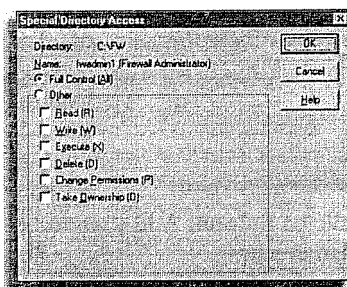
setele de validare Replace Permissions on Subdirectories și Replace Permissions on Existing Files, tuturor fișierelor și subdirectoarelor care se găsesc sub dosarul fw li se modifică permisiunile.

Acest exemplu a arătat cum să adăugați sau să ștergeți permisiuni standard pentru utilizatori sau grupuri selectate. Dacă vă uitați din nou la figura 6.7, puteți vedea că în caseta în care sunt listate permisiunile pentru utilizatori sau grupuri este afișată inițial permisiunea standard Full Control, iar apoi, între paranteze, alte două permisiuni: (All) și (All). Amintiți-vă că pentru directoare (sau dosare) există două seturi de permisiuni. Aceste ultime două șiruri de permisiuni indică permisiunile speciale pentru director și permisiunile speciale care trebuie aplicate fișierelor create în director.

Dacă doriți să modificați permisiunea pentru un utilizator sau un grup care are deja acces, puteți efectua această operație din caseta de dialog Directory Permissions. Nu trebuie decât să selectați utilizatorul executând clic o singură dată pe el și apoi să folosiți meniul Type of Access pentru a selecta noua valoare de permisiune pentru acel utilizator sau grup. Veți observa că, pe lângă permisiunile standard pe care aveți posibilitatea să le selectați din caseta de dialog Add Users and Groups, meniul Type of Access din caseta de dialog Directory Permissions vă permite să selectați și opțiunea Special Directory Access (Acces special la director). Iată cum puteți utiliza aplicația Explorer pentru a modifica permisiunile pentru un obiect folosind permisiunile speciale în locul permisiunilor standard.

FIGURA 6.10

Selectați permisiunile speciale pe care doriți să le aplicați directorului folosind această casetă de dialog.



În figura 6.10 puteți vedea caseta de dialog Special Directory Access, utilizată pentru a specifica permisiunile speciale pe care doriți să le aplicați directorului.

După ce selectați una sau mai multe permisiuni speciale pe care doriți să le aplicați, executați clic pe butonul OK. După ce reveniți în caseta de dialog Directory Permissions, veți observa că textul Full Access a fost înlocuit cu Special Access, iar prima valoare de permisiune specială, pentru accesul la director, a fost modificată. Pentru a efectua modificări în al doilea câmp de permisiuni speciale sau pentru cele care vor fi aplicate

fișierelor create în director, folosiți meniul Type of Access pentru a selecta opțiunea Special Directory Access. Dintr-o casetă de dialog similară cu cea prezentată în figura 6.10, puteți să selectați permisiunile speciale care trebuie aplicate fișierelor create în director.

Atunci când folosiți caseta de dialog Directory Permissions pentru a schimba permisiunile pentru un director existent, noile permisiuni au efect numai pentru fișierele noi create în director. Dacă în director există deja fișiere, trebuie să folosiți casetele de validare Replace Permissions pe care le-ați utilizat în exemplu, dacă doriți să propagați modificările permisiunilor și la fișierele și/sau subdirectoarele existente.

Configurarea auditării și a înregistrării în jurnal

După ce ați stabilit permisiunile la resurse pentru resursele care vor fi necesare gazdei bastion, ar trebui să vă asigurați că facilitățile oferite de sistemul de operare pentru înregistrarea în jurnal și auditare sunt configurate corect. Acesta este un subiect atât de important, încât i-a fost dedicat un întreg capitol, și anume capitolul 8, „Tehnici de monitorizare și auditare a sistemelor de operare“.

Indiferent de protecțiile pe care le configurați folosind permisiuni pentru a restricționa accesul la fișiere și directoare, nu veți fi sigur că metodele dumneavoastră funcționează până când nu treceți la etapa de monitorizare a situației. Fișierele jurnal și tehnicile de monitorizare, cum ar fi demonul syslogd pentru sistemele UNIX și aplicația Windows NT Event Viewer, trebuie să fie înțelese și implementate corespunzător. În plus, trebuie să stabiliți proceduri de revedere frecventă a datelor colectate, astfel încât să puteți detecta cu rapiditate orice activitate suspectă. Chiar dacă aceste aspecte sunt valabile pentru securitatea tuturor sistemelor din rețeaua dumneavoastră, pentru o gazdă bastion sunt și mai importante.

Rularea unui software intermediar pe o gazdă bastion

Modul uzual de folosire a unei gazde bastion presupune oferirea unui tip de serviciu intermediar în Internet utilizatorilor din rețeaua internă protejată. Aplicațiile intermediare pot include utilitare TCP/IP clasice, cum ar fi FTP, Telnet, protocoale Internet mai noi, cum ar fi HTTP, sau funcții importante pentru afaceri, cum ar fi poșta electronică (SMTP).

Vezi și

➤ Pentru mai multe informații despre serviciile intermediar și porțile de aplicație, vezi capitolul 7, „Porți de aplicații și servere intermediar“, la pagina 132.

În acest capitol am discutat necesitatea de a face gazda bastion cât mai sigură posibil, lăsând pe calculatorul respectiv numai componentele de care are nevoie pentru a-și îndeplini funcția în cadrul firewall-ului. Această funcționalitate va fi determinată de aplicațiile software intermediare pe care le alegeți să ruleze. Atunci când bugetul vă permite, este o idee mai bună să folosiți mai multe servere intermediare pentru a oferi mai multe servicii decât să faceți o singură gazdă responsabilă pentru mai multe servicii. Utilizând câte o singură gazdă bastion pentru fiecare serviciu important, puteți să ajutați la împărțirea sarcinilor și, probabil, la îmbunătățirea timpului de răspuns pentru utilizatori

Folosind mai multe gazde pentru a oferi același serviciu, puteți, de asemenea, să echilibrați încărcarea serverelor. De exemplu, atât Microsoft Proxy Server, cât și serverul intermediar SQUID oferă suport pentru comunicații între serverele intermediare astfel încât solicitările să poată fi satisfăcute folosind o rețea distribuită, ierarhică, de servere. Într-o rețea mare, o ierarhie de servere intermediare poate fi mai eficientă în ceea ce privește răspunsul la solicitările clienților decât un singur server.

Utilizarea mai multor servere înseamnă creșterea numărului de activități de gestionare a sistemului dumneavoastră. Pe de altă parte, fiecare sistem ar trebui să fie mai simplu de întreținut dacă se ține seama de faptul că va fi folosit pentru un singur serviciu intermediar. Un alt avantaj al utilizării mai multor servere este acela că, în cazul în care un server se defectează, celelalte servicii Internet nu sunt afectate. Dacă folosiți mai multe servere pentru același serviciu, pierderea unuia înseamnă că puteți să asigurați în continuare o conexiune pentru clienți până când serverul defect revine la regimul de lucru normal.

Compromiterea unei gazde bastion

Deoarece o gazdă bastion este plasată mai aproape de Internet decât majoritatea sistemelor din rețeaua dumneavoastră, este normal că această gazdă are șanse mai mari de a fi infiltrată de intruși. Din acest motiv am dedicat un capitol întreg discuției despre crearea unui sistem foarte securizat. Deși puteți face sarcina unui hacker mai dificilă, nu există o metodă 100% garantată de prevenire a tuturor formelor de atac. Această afirmație este adevărată mai ales pentru că permanent sunt dezvoltate noi metode de atac.

Prin folosirea unor măsuri bune de auditare ar trebui să fiți capabil să detectați cu rapiditate momentul în care a avut loc o intruziune. Însă, indiferent cât de repede vă dați seama că ceva nu este în regulă, s-ar putea să nu fie suficient de repede pentru a evita pagube ulterioare. S-ar putea ca intrusul să fi modificat deja fișierele de sistem sau să fi plantat alte aplicații, cum ar fi cele de tip cal troian. Este posibil ca intrusul să modifice fișiere asociate cu un serviciu intermediar de aplicație. Din aceste motive, nu puteți doar să schimbați o parolă și să reintroduceți calculatorul gazdă în serviciu. Trebuie să începeți din nou de la zero și să evaluați gazda bastion pentru a fi sigur că este exact ceea ce dumneavoastră credeți că este.

Cu toate că ar putea fi tentant să restaurați foarte simplu gazda bastion folosind o bandă cu o copie de siguranță recentă, această metodă nu este la fel de sigură ca pornirea de la zero folosind programe cunoscute de configurare a aplicațiilor. Dacă gazda bastion a fost compromisă, nu puteți fi sigur 100% de momentul în care a început atacul. De exemplu, dacă gazda s-a blocat, aceasta se datorează unui program descărcat recent pe calculatorul respectiv sau unui program de tip cal troian care așteaptă de câteva luni un semnal de declanșare?

Există câteva utilitare bune care vă pot ajuta în această analiză, cum ar fi TripWire. Pentru mai multe informații despre programe de acest gen, vezi anexa B, „Alte instrumente de securitate pe care le puteți folosi”.

Când gazda bastion este compromisă, toate celelalte gazde care se găsesc în zona DMZ trebuie analizate. Dacă un sistem a fost penetrat, este foarte probabil ca informațiile obținute din această pătrundere să poată fi utilizate pentru o penetrare ulterioară a rețelei. Când o gazdă bastion este compromisă, ar trebui să examinați toate celelalte gazde care

interacționează cu gazda bastion, cum ar fi ruterele și celelalte porți, pentru a vă asigura că ați determinat dimensiunea reală a pagubelor.

Rezumat

Configurarea unui sistem pentru a fi utilizat ca gazdă bastion presupune că trebuie să parcurgeți toate etapele necesare pentru a vă asigura că gazda este bine protejată de aproape orice pericol pe care îl anticipați (și de o mulțime de lucruri la care nu vă așteptați). Aceasta înseamnă să folosiți protecțiile interne ale resurselor, oferite de sistemul de operare de bază, și să vă asigurați că sistemul de operare a fost instalat corect. În capitolul următor vom analiza modul în care funcționează serviciile intermediare pentru care veți folosi gazda bastion.

Porți de aplicații și servere intermediar

- Utilizarea serverelor intermediare
- Intermediare clasice și transparente
- Translatoare de adrese de rețea (NAT)
- Ecranarea și blocarea conținutului
- Facilități de înregistrare în jurnal și de avertizare
- Considerații referitoare la client

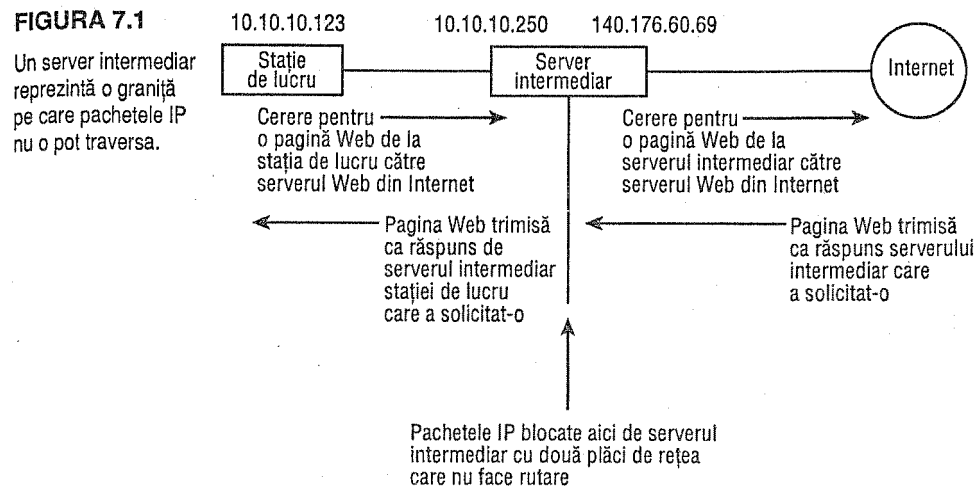
Utilizarea serverelor intermediare

Dacă filtrele de pachete operează la nivelul transport de rețea prin inspectarea informațiilor de antet corespunzătoare protocolului IP și altor protocoale, serverele intermediare lucrează la nivelul aplicație și pot fi utilizate pentru o varietate de servicii de rețea. Un server intermediar, prin care trebuie să circule toate pachetele de rețea pentru o anumită conexiune, oferă o poartă între client și server. Un alt termen utilizat uzual este *poartă de aplicație* (*application gateway*). Un server intermediar nu transferă pachetele IP între rețele interne și externe, așa cum procedează filtrele de pachete, ci recepționează o cerere de la un client și face în continuare o cerere către server în interesul clientului. Între client și server nu sunt transferate pachete IP. Serverul intermediar este poziționat în mijlocul conexiunii și discută cu ambele părți pentru a media conexiunea.

Una dintre principalele diferențe între un filtru de pachete și un server intermediar este aceea că un server intermediar trebuie să înțeleagă aplicația. Un filtru de pachete poate fi programat să permită sau să interzică trecerea pachetelor de rețea pe baza unei cantități limitate de informații găsite în antetul pachetului. Serverul intermediar este specific unei aplicații și poate fi programat pentru a permite sau a interzice accesul la un serviciu pe baza funcțiilor pe care dorește să le efectueze clientul.

În figura 7.1 puteți vedea cum operează un server intermediar pentru a bloca traficul IP, împiedicându-l să circule între rețeaua dumneavoastră și Internet. Utilizatorul care navighează în Internet de la propria stație de lucru cere o pagină Web din Internet. Deoarece browserul utilizatorului a fost configurat să trimită cereri HTTP unui server intermediar, solicitarea nu ajunge niciodată direct la serverul Web.

FIGURA 7.1



Serverul intermediar este cel care primește cererea prin adaptorul său de rețea conectat la rețeaua locală. Serverul intermediar nu rutează (sau retransmite) pachetul IP care conține cererea către serverul destinație din Internet. Aplicația intermediară care rulează pe serverul intermediar consultă un set de reguli, configurate de administrator, pentru a decide dacă cererea este permisă. În caz afirmativ, serverul intermediar formulează o cerere pentru pagina respectivă, utilizând ca sursă a cererii adresa celui alt adaptor de rețea propriu (care este conectat la Internet). Când serverul Web din Internet primește cererea, poate doar să presupună că serverul intermediar este clientul care solicită pagina și îi trimite acestuia datele.

Când serverul intermediar recepționează pagina Web solicitată, nu transferă pachetele IP înapoi către clientul inițiator al cererii, ci efectuează câteva verificări în datele returnate, după cum a fost configurat de administrator. Dacă totul este în regulă, serverul intermediar creează noi pachete IP cu adresa adaptorului de rețea local și returnează clientului datele din pagina Web.

După cum puteți vedea, blocarea traficului IP nu este singurul avantaj de care beneficiați prin utilizarea unui server intermediar. Puteți să folosiți acest server și pentru a executa o serie de verificări pe baza tipului de cerere și a conținutului datelor returnate. În plus, pe baza unui set de reguli configurat de dumneavoastră, puteți programa serverul intermediar să permită sau să refuze datele.

Veți avea nevoie de câte o aplicație server intermediar pentru fiecare tip de serviciu de rețea la care veți permite accesul clienților prin firewall. Aplicațiile intermediare standard sunt numeroase pentru utilitate TCP/IP obișnuite, cum ar fi FTP și Telnet, și pentru servicii mai răspândite, cum este HTTP. S-ar putea să nu găsiți software intermediar pentru serviciile mai noi sau pentru cele care sunt folosite mai rar. Cu toate că există soluții intermediare generale, ele nu oferă același grad de securitate pe care îl oferă un software intermediar specific aplicației.

Serverele intermediare pot opera în ambele direcții. La fel cum puteți folosi un server intermediar pentru a controla ce utilizatori din rețeaua dumneavoastră au permisiunea de a

face cereri în Internet, puteți să utilizați un server intermediar pentru a decide ce utilizatori sau gazde din exterior vor avea dreptul de a trimite solicitări serverelor din rețeaua proprie. În oricare dintre situații, nici un pachet IP nu trece între cele două rețele și puteți permite sau interzice cererile prin configurarea unui set de reguli.

Dezactivarea rutării pe serverul intermediar

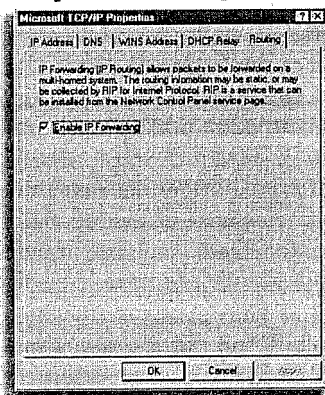
Atunci când configurați un calculator gazdă cu două plăci de rețea pentru a fi folosit ca server intermediar, asigurați-vă că dezactivați rutarea între cele două adaptoare de rețea. Această caracteristică este în mod obișnuit activată. Prin dezactivarea retransmiterii IP sau a rutării de către gazdă, toate conexiunile client/server vor fi forțate să treacă prin aplicațiile intermediare disponibile sau vor fi blocate.

Windows NT și multe versiuni de UNIX efectuează în mod prestabilit rutarea între adaptoare. În cazul sistemului Windows NT, puteți dezactiva această funcție foarte simplu:

1. Executați clic pe Start, Programs, Control Panel.
2. Executați dublu clic pe miniaplicația Network.
3. Selectați foaia de proprietăți Protocols.
4. Executați dublu clic pe opțiunea TCP/IP Protocol (sau evidențiați TCP/IP cu un clic și apoi executați clic pe butonul Properties).

FIGURA 7.2

Ștergeți semnul din caseta de validare Enable IP Forwarding pentru a dezactiva rutarea între adaptoarele unui calculator gazdă Windows NT cu două plăci de rețea.



5. În caseta de dialog afișată (vezi figura 7.2), deselectați caseta de validare denumită Enable IP Forwarding (Permite retransmiterea IP).
6. Reporniți calculatorul pentru ca această setare să aibă efect.

Dacă utilizați un sistem UNIX, metoda va varia de la o variantă de sistem la alta și poate fi diferită chiar pentru versiuni diferite ale aceluiași tip de UNIX. De exemplu, în Solaris 2.4 și versiunile anterioare, adăugați

următoarea linie de cod la sfârșitul fișierului /etc/init.d/inetinit:

```
-set /dev/ip ip_forwarding 0
```

Pentru Solaris 2.5 însă, nu trebuie decât să aplicați comanda touch fișierului etc/norouter.

Vezi și

- Pentru mai multe informații despre configurarea unei gazde cu două plăci de rețea pentru a fi utilizată de aplicațiile intermediare, vezi capitolul 6, „Utilizarea unei gazde bastion”, la pagina 112.

Retransmiterea IP în Windows 2000

Retransmiterea IP este dezactivată în mod prestabilit în sistemul Windows 2000. Pentru a activa această funcție, trebuie să editați fișierul Registry.

Ce este touch?

Această comandă UNIX este folosită pentru a stabili accesul și perioadele de modificare ale unui fișier. Dacă fișierul căruia îi aplicați comanda touch nu există, va fi creat.

Avantaje și dezavantaje ale serverelor intermediare

Serverele intermediare nu reprezintă decât o componentă a unui firewall bun și, la fel ca filtrele de pachete, au părți bune și părți rele. Prin combinarea celor două componente, puteți acoperi mai multe elemente de securitate și vă puteți proteja mai bine rețeaua. Iată câteva avantaje pe care le puteți obține prin utilizarea unui server intermediar:

- Ascunderea informațiilor de rețea despre clienții sau serverele din rețeaua protejată.
- Existența unui singur punct critic în rețea de unde puteți controla accesul la serviciile de rețea între rețeaua protejată și Internet. Chiar dacă aplicația intermediară se blochează sau se defectează, pe o gazdă bastion configurată corespunzător nu mai rămâne nici un mecanism care să permită trecerea traficului.
- Serverele intermediare pot fi configurate pentru a înregistra în jurnale informații despre serviciile oferite și pentru a vă alerta în cazul activităților suspecte și încercărilor de acces neautorizat.
- Unele servere intermediare pot ecrana conținutul datelor returnate și pot bloca accesul la anumite situri. De asemenea, ele pot bloca și datele care conțin viruși cunoscuți sau alte obiecte nesigure.

Între dezavantaje se numără următoarele:

- Cu toate că un server intermediar asigură o singură locație de control al accesului, acesta devine și un punct critic de defectare.
- Fiecare serviciu de rețea va necesita propria aplicație server intermediar. Există și soluții generale, însă nu oferă același nivel de securitate.
- Ar putea fi nevoie de modificarea sau reconfigurarea clienților pentru ca aceștia să folosească un server intermediar.

Intermediare clasice și transparente

În documentul RFC 1919, autorul acestuia descrie și compară două tipuri fundamentale de intermediare și le numește *intermediare clasice* și *intermediare transparente*.

Intermediare clasice

După cum sugerează și numele, un server intermediar clasic se referă la primul tip de server intermediar care a fost dezvoltat. Într-un anumit sens, acest tip de intermediar nu este decât un program care este plasat între client și server. Serverul intermediar obligă clientul de la capătul conexiunii să se autentifice intermediarului înainte ca acesta să înceapă transferul de date înainte și înapoi. De exemplu, un utilizator care folosește un intermediar clasic pentru utilitarul FTP ar putea să îl utilizeze ca pe o țintă a comenzii FTP,

să se autentifice la serverul intermediar și apoi să informeze serverul care este ținta reală a conexiunii.

Problema acestui tip de server intermediar este că presupune operații suplimentare pentru client. De exemplu, atunci când se folosește FTP direct, fără intermediar, etapele sunt simple:

1. Utilizatorul execută comanda client FTP, de genul `ftp www.twoinc.com`.
2. Serverul cere un nume de utilizator, utilizatorul răspunde.
3. Serverul cere o parolă, utilizatorul răspunde.
4. Utilizatorul execută comenzile pentru a trimite sau a recepționa fișiere, și așa mai departe.
5. Serverul răspunde la comenzi recepționând fișierele de la aplicația client a utilizatorului sau trimițând fișiere către aplicația clientului.

Folosind un intermediar clasic, situația devine puțin mai complicată:

1. Utilizatorul execută comanda client FTP, de genul `ftp proxyserver.twoinc.com`.
2. Serverul cere un nume de utilizator, utilizatorul răspunde.
3. Serverul cere o parolă, utilizatorul răspunde.
4. Utilizatorul indică serverului intermediar destinația reală a conexiunii FTP, de obicei într-un format similar cu `username@target.com`. În acest exemplu, `username` este un nume valid de utilizator de pe sistemul destinație, iar `target.com` este ținta finală a sesiunii FTP.
5. Serverul intermediar retransmite informațiile de conectare către destinație și, dacă autentificarea s-a încheiat cu succes, informează aplicația client că utilizatorul poate să execute comenzi FTP.
6. Serverul intermediar recepționează comenzile FTP de la software-ul client al utilizatorului și le retransmite către serverul destinație.
7. Serverul destinație răspunde la comenzile primite de la serverul intermediar ca și când ar fi clientul său și returnează datele către serverul intermediar, în funcție de comenzile lansate de client.
8. Serverul intermediar retransmite datele recepționate de la serverul destinație înapoi la aplicația client a utilizatorului.

Din acest exemplu, puteți vedea că pentru serverul destinație de la capătul conexiunii, serverul intermediar arată ca și cum ar fi un alt client FTP. Pentru clientul FTP al utilizatorului final, serverul intermediar pare să fie chiar serverul destinație. Deoarece serverul intermediar este situat la mijloc, sunt necesare operațiile suplimentare de autentificare a utilizatorului la serverul intermediar și apoi comanda prin care se indică serverului intermediar care este destinația dorită. Deoarece autentificarea este executată și pe serverul intermediar și pe serverul destinație, utilizatorul este încărcat cu comenzi suplimentare.

Pentru majoritatea utilizatorilor, acest proces s-ar putea să nu pară foarte complex. Însă folosirea unui server intermediar de acest tip presupune ca utilizatorul să fie instruit pentru întreținerea sa. Nu toate aplicațiile server intermediar funcționează la fel, astfel că utilizarea intermediarului Telnet s-ar putea să nu fie exact la fel cu utilizarea unui intermediar FTP și așa mai departe. Etapele suplimentare și instruirea utilizatorilor fac din acest tip de server intermediar o soluție acceptabilă, dar nu perfectă.

Vezi și

- *Pachetul TIS Internet Firewall Toolkit (FWTK) conține câteva servere intermediare care funcționează în maniera unui intermediar clasic. Pentru informații despre FWTK și intermediarele livrate în acest pachet, vezi capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)”, la pagina 217.*

Serverul intermediar blochează traficul IP direct

Rețineți, de asemenea, din acest exemplu că software-ul client real nu comunică niciodată direct cu gazda destinație reală care oferă serviciul respectiv. Mai precis, un pachet IP trimis de gazda clientului nu ajunge niciodată la serverul destinație. Destinația finală a acestui pachet este serverul intermediar. Acesta interpretează informațiile din pachet și apoi configurează o conexiune între el și serverul destinație. Astfel, în realitate sunt stabilite două conexiuni: una între client și serverul intermediar și a doua între serverul intermediar și serverul destinație. Această situație previne trimiterea unui pachet eronat în rețea. Amintiți-vă că nu toate metodele de atac cer ca informațiile să fie retransmise înapoi la atacator. Uneori este suficient doar să fie trimis un pachet în interiorul rețelei pentru a declanșa o acțiune care poate fi exploatată de atacator printr-un alt canal.

Intermediare transparente

Pentru ca aplicațiile intermediare să fie mai ușor de gestionat și mai ușor de folosit de către utilizatorul final, aveți nevoie de o aplicație intermediară care să fie transparentă pentru utilizator. Astfel, nu mai sunt necesare comenzi suplimentare, iar utilizatorul nici nu ar trebui să știe că folosește un server intermediar. Din punctul de vedere al utilizatorului, un intermediar transparent funcționează la fel ca o conexiune directă. Acest tip de intermediar ar trebui să fie mult mai ușor de implementat, deoarece utilizatorul nu mai trebuie să fie instruit asupra modului de folosire. Utilizatorul nici nu ar trebui să știe că există un server intermediar.

În loc să folosească serverul intermediar ca destinație a comenzii FTP, utilizatorul execută comanda având serverul țintă real ca parametru în linia de comandă. Deoarece se găsește pe traseul dintre utilizator și serverul destinație și a fost programat să intercepteze anumite tipuri de trafic de rețea, serverul intermediar poate să evalueze o cerere și să decidă dacă este cazul să o permită (sau să o interzică). Aceasta înseamnă că un client care trimite o cerere FTP crede că se află în comunicație directă cu serverul destinație. Stiva TCP/IP a serverului intermediar a fost modificată pentru a prelua pachetele de rețea destinate propriei adrese IP, ca și pachetele IP care sunt trimise către serverele țintă protejate de acel server intermediar.

Deoarece serverul intermediar transparent interceptează ceea ce altfel ar fi o conexiune directă, poate să determine adresa serverului țintă evaluând pachetul interceptat. Nu este nevoie ca utilizatorul să introducă numele serverului destinație, așa cum se procedează în cazul unui server intermediar clasic.

Utilizatorul trebuie să se autentifice pe serverul țintă, la fel ca într-o conexiune directă. Însă serverul intermediar este poziționat la mijlocul acestei conexiuni și poate permite sau interzice anumite acțiuni. De exemplu, ar putea să permită utilizatorului să obțină fișiere de pe serverul țintă (comanda GET), dar, în același timp, să interzică utilizatorului să trimită fișiere către serverul țintă (comanda PUT). Serverul intermediar poate asigura controlul accesului hotărând cine și ce acțiuni sunt permise și poate oferi funcțiile de înregistrare în

jurnal și de alertare, la fel ca un server intermediar clasic. Însă pentru utilizator, acest proces este transparent, operând la fel ca o conexiune directă.

Totuși, serverul intermediar transparent nu ascunde informațiile IP din cele două părți ale conexiunii intermediare. Clientul trebuie să cunoască adresa IP a serverului țintă. Dacă folosiți un intermediar pentru a permite gazdelor din exterior să realizeze o conexiune cu un server din interiorul rețelei dumneavoastră, serverul din interior crede în continuare că respectivul client este serverul intermediar. Însă clientul extern știe adresa IP a serverului. O soluție la această problemă este plasarea serverelor într-o subrețea separată din rețeaua internă, de genul zonei DMZ. În acest mod, orice atacator care încearcă să hărțuiască aceste servere nu va primi nici o informație despre restul rețelei, care se găsește de cealaltă parte a zonei DMZ. Amintiți-vă că gazdele pe care le plasați într-o zonă DMZ pentru a oferi servicii sunt denumite în general gazde bastion și trebuie să fie securizate cu strictețe deoarece sunt cele mai vulnerabile gazde din rețea.

Vezi și

- Pentru mai multe informații despre zona demilitarizată (DMZ) și modul în care se potrivește într-o arhitectură de firewall, vezi capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, la pagina 75.

Indiferent de metoda folosită, un lucru important pe care trebuie să vi-l amintiți este acela că, în cazul în care aplicațiile intermediare nu au fost configurate pentru a permite utilizatorului (sau gazdei) să stabilească o conexiune prin firewall, conexiunea va fi interzisă. Chiar dacă filtrul de pachete funcționează analizând informațiile din antetul pachetului (cum sunt adresa și numărul de port), aplicația server intermediar a fost scrisă pentru a înțelege acțiunile efective executate de serviciul de rețea. Acest server poate fi programat pentru a permite sau a interzice comunicațiile prin conexiune în funcție de anumite acțiuni.

Intermediarele clasice pot ascunde informațiile DNS referitoare la rețeaua dumneavoastră

Un lucru important ar trebui să devină evident celor care folosesc aplicații intermediare clasice: clientul nu trebuie să cunoască decât numele serverului intermediar și numele sistemului destinație cu care dorește să stabilească o conexiune. Din punctul de vedere al clientului, va fi necesară traducerea numelui în stil DNS al serverului intermediar într-o adresă IP propriu-zisă, înainte de a putea fi încercată conexiunea efectivă. Însă nu este obligatoriu ca aplicația client să translateze și numele serverului destinație într-o adresă IP. Deoarece clienții vor avea nevoie să cunoască doar numele sistemului destinație, nu este necesar să fie publicate informații DNS despre rețeaua dumneavoastră internă. Intermediarul vă ajută să ascundeți informațiile despre rețeaua internă de lumea exterioară.

O metodă uzuală de instalare a sistemului DNS în acest tip de situație este folosirea unui server DNS intern care să poată rezolva numele clienților din rețeaua internă. Acest server DNS intern nu asigură rezolvarea numelor pentru gazdele din afara rețelei interne. Un alt server DNS este configurat pentru a rezolva numele pentru gazdele din exterior.

Vezi și

- Pentru mai multe informații despre serviciul DNS (Domain Name Service) și modul de configurare a acestui serviciu, vezi capitolul 2, „Introducere în suita de protocoale TCP/IP”, la pagina 26.

Un server intermediar transparent nu oferă această separare. Într-un intermediar transparent, sistemul client trebuie să cunoască adresa IP efectivă a serverului destinație. Ca urmare, trebuie să fie capabil să rezolve numele de gazdă al serverului destinație într-o adresă IP; din acest motiv, unele informații despre rețeaua internă trebuie făcute publice de un server DNS.

Crearea unei aplicații intermediare personalizate

Unele servere intermediare vă permit să creați un intermediar personalizat pentru servicii. De exemplu, în pachetul TIS Firewall Toolkit (prezentat în capitolul 14), care include aplicațiile intermediare standard, puteți să folosiți poarta plug-gw pentru a crea conexiuni intermediare pentru servere cunoscute și sigure din exterior. Însă această metodă nu vă permite să efectuați nici o analiză a datelor transferate, deci nu este un intermediar adevărat, ci acționează mai mult pentru a vă permite să faceți excepții de la politica de securitate prin firewall și să cuplați două servere/porturi astfel încât ele să poată dialoga prin firewall. Acest tip de intermediar vă permite să specificați ce utilizatori sau gazde pot folosi serviciile din cealaltă parte a firewall-ului. Poate să execute și sarcini de înregistrare în jurnal și de alertare, la fel ca orice alt server intermediar bun. Însă este o poartă de tip totul sau nimic, iar în multe cazuri nu este de dorit din punctul de vedere al securității.

- Dacă doriți să aflați mai multe despre plug-gw, citiți capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)”, la pagina 217.

Utilizarea unui fișier hosts

Mai există o metodă pe care o puteți folosi pentru a permite clienților din Internet să rezolve numele de server din rețeaua dumneavoastră internă: fișierul `etc/hosts`. Acest fișier, care conține linii ce mapează adresele IP la nume de gazde, a fost o metodă obișnuită pentru rezolvarea numelor la începutul utilizării stivei TCP/IP. Dezavantajul major al acestei soluții este acela că, dacă schimbați o adresă IP sau un nume de gazdă, trebuie să mergeți la fiecare client și să modificați fișierul `hosts`. Pentru un număr mare de gazde, această activitate poate consuma foarte mult timp. Utilizând un server DNS, nu trebuie să efectuați modificarea decât o dată. Dacă folosiți un intermediar transparent și există puțini clienți în afara rețelei dumneavoastră, utilizarea unui fișier `hosts` poate fi o soluție acceptabilă. Totuși, nu este o soluție practică în situația în care oferiți un serviciu public (de genul unui sit FTP anonim).

Translatoare de adrese de rețea (NAT)

Network Address Translator (NAT) este un serviciu intermediar foarte răspândit. Una dintre cele mai importante funcții de securitate executate de un firewall este de a ascunde persoanelor din exterior informațiile despre rețeaua internă. Aceste informații includ adresarea TCP/IP și datele de configurare pentru stațiile de lucru și serverele din rețea. Pentru a ascunde informațiile despre gazdele dumneavoastră, o aplicație NAT folosește propria adresă IP (sau un interval de adrese IP) atunci când face cereri în Internet în

interesul clienților din rețeaua internă. În rețeaua dumneavoastră protejată, clienții comunică utilizând adresele IP atribuite efectiv. Atunci când este trimisă o cerere prin firewall, aplicația NAT înlocuiește cu propria sa adresă câmpul cu adresa sursă. Când sosește un răspuns la aplicația NAT, aceasta înlocuiește propria adresă din câmpul destinație cu adresa clientului care a făcut cererea.

Un lucru important care trebuie remarcat aici este acela că sunt multe metode folosite pentru a implementa serviciul NAT. Unele translatoare NAT utilizează *atribuiri statice de adrese*, în care adresa unui client din rețeaua internă este legată la o adresă IP fixă folosită de NAT în lumea exterioară. Translateoarele NAT care folosesc *atribuirea dinamică a adreselor* pot atribui o adresă IP pentru a fi utilizată în rețeaua externă atunci când clientul formulează o solicitare care trece dincolo de serverul intermediar. După ce se termină sesiunea client, sau după trecerea unui anumit timp, adresa validă în lumea exterioară este returnată unui domeniu de adrese și așteaptă următoarea atribuire.

NAT poate lucra într-un mod unidirecțional, în care clienților din rețeaua internă le este atribuită o adresă de către NAT atunci când sunt inițiate sesiuni către exterior, sau în mod bidirecțional, în care adresele IP destinație sosite din exterior pot fi modificate pentru a trimite un pachet unui server din rețeaua internă folosind o adresă diferită.

Porți de nivel aplicație și de nivel circuit

Serverele intermediare sunt proiectate în general pentru a lucra la nivelul aplicației, în timp ce filtrele de pachete lucrează la nivelul rețelei. În literatura de specialitate puteți găsi alți doi termeni utilizați pentru a face referire la intermediari. O poartă de nivel aplicație este un server intermediar care înțelege modul de lucru intern al protocolului sau serviciului (aplicației) folosit(e). O poartă de nivel circuit, cum este *plug-gw*, este generală și nu înțelege serviciul sau protocolul pentru care este oferit un serviciu intermediar. Porțile de nivel circuit sunt configurate de administrator pentru a corecta o conexiune particulară prin firewall. Cu toate că porțile de nivel circuit nu vă permit să controlați funcțiile care pot fi utilizate, oferă capabilități de înregistrare în jurnal și de avertizare.

Translateoare NAT de bază

Conceptul de traducere de adresă de rețea, despre care am discutat până în acest moment, este referit uzual ca traducere NAT de bază. Această implementare presupune ca una sau mai multe adrese de rețea Internet valide să fie atribuite serverului NAT astfel încât acesta să le folosească pentru a stabili conexiuni pentru mai mulți clienți din rețeaua internă. Rezultă de aici că numărul de adrese IP valide pe care trebuie să le rezervați pentru a fi utilizate de NAT trebuie să fie egal cu numărul de sesiuni active către exterior, în orice moment. Dacă atribuiți 10 adrese IP pentru NAT, numai 10 clienți din rețeaua internă vor putea stabili simultan conexiuni în exterior.

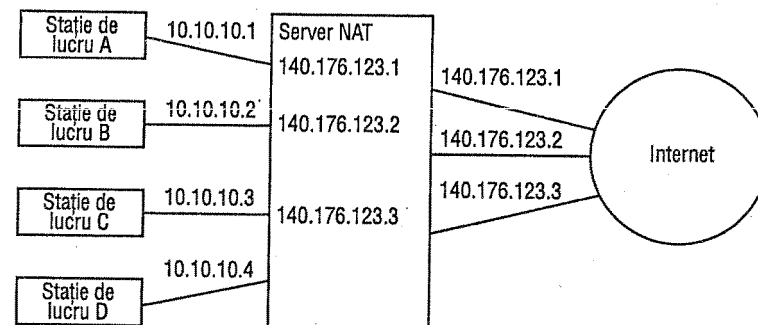
Figura 7.3 prezintă un exemplu de astfel de situație. Stația de lucru A are atribuită adresa 10.10.10.1 pentru adaptorul de rețea propriu. Atunci când face o cerere de conexiune în Internet, serverul NAT folosește adresa 140.176.123.1 din domeniul său de adrese pentru a realiza conexiunea efectivă.

Când stațiile de lucru B și C efectuează cereri de conexiuni, serverul NAT folosește următoarele două adrese din domeniu. Însă când stația de lucru D încearcă o conexiune Internet, nu mai este nici o adresă disponibilă, iar cererea va fi refuzată. Dacă se utilizează traducerea NAT statică, stația de lucru D nu va fi capabilă să realizeze niciodată cu succes

o cerere de conexiune în Internet. Dacă se folosește traducerea NAT dinamică, stația de lucru D poate încerca din nou mai târziu, după ce o altă stație de lucru a returnat o adresă în domeniu.

FIGURA 7.3

Translatearea NAT de bază folosește o metodă de traducere a adreselor unu-la-unu atunci când permite clienților să utilizeze domeniul de adrese.



Dacă utilizarea conexiunilor către exterior este limitată, traducerea NAT de bază ar putea fi ideală pentru rețeaua dumneavoastră. Dacă aveți un număr mare de clienți care trebuie să stabilească simultan conexiuni și nu dispuneți de un număr suficient de mare de adrese IP valide pentru a folosi traducerea NAT, această metodă nu va funcționa.

Translatearea portului de adresă de rețea (NAPT)

În capitolul 2 am discutat despre conceptul de soclu, combinația dintre o adresă IP și un număr de port, utilizată pentru a identifica în mod unic un punct final într-o comunicație TCP sau UDP. Regula standard (care nu este respectată întotdeauna) spune că porturile 0-1023 sunt rezervate pentru a fi utilizate de servere, iar cele cu valori mai mari de 1024 sunt disponibile pentru clienți sau pentru alte utilizări. Să luăm, de exemplu, o conexiune TCP: clientul va trimite o cerere către un server și include în informațiile de antet o adresă IP destinație și un număr de port. De asemenea, clientul va mai include adresa IP sursă proprie și un număr de port. Numerele de porturi nu trebuie să corespundă între ele, ci trebuie să identifice în mod unic conexiunea astfel încât calculatorul gazdă să poată ține o evidență a aplicației care comunică și a aplicației de pe celălalt calculator gazdă.

Numărul de port folosit de client ca destinație a pachetului este de obicei interpretat de serverul destinație pentru a indica serviciul care trebuie folosit. De exemplu, serverele Telnet „ascultă” în general portul 23. Portul sursă transmis de client serverului poate să varieze ca valoare. Nu este necesar decât ca serverul Telnet să știe care este acel număr de port și să îl folosească atunci când îi trimite răspunsuri clientului.

Probabil vă dați seama care este sensul discuției. Pentru a extinde și mai mult numărul de conexiuni permise către exterior, fără a fi nevoie de creșterea numărului de adrese IP alocate exclusiv pentru a fi utilizate de NAT, a fost creată o formă nouă de traducere NAT, denumită traducerea portului de adresă de rețea (Network Address Port Translation, sau NAPT), care poate înlocui adresa IP a clientului și numărul de port sursă al clientului. Utilizând această metodă, o singură adresă IP validă în Internet poate fi distribuită mai multor clienți din rețeaua LAN internă prin simpla schimbare a numărului de port sursă. Serverul NAT ține evidența clienților actualizând un tabel care translatează

conexiunea clientului către o adresă IP din exterior și un număr de port unic pentru acea adresă IP.

În unele implementări ale NATP, mai sunt folosiți termenii Port Address Translation (PAT) (translatarea adresei de port) și NAT Overloading.

Rezultatul este că o singură adresă IP poate fi folosită în Internet pentru a reprezenta un număr mare de clienți din rețeaua internă.

Alte date care pot fi modificate de translatarea NAT

Pe lângă schimbarea adresei IP sursă și, posibil, a numărului de port sursă, nu uitați că mai există și alte câmpuri care trebuie modificate. Acestea sunt câmpurile cu sumele de control din anteturile pachetelor. Înlocuirea unei adrese IP va impune și modificarea sumei de control a antetului respectiv. Dacă uitați această operație, pachetul va fi respins la celălalt capăt al conexiunii. Stiva TCP/IP de la capăt va stabili că pachetul a fost probabil modificat sau corupt într-un anumit fel în timpul transmisiei. Serverele NAT trebuie să efectueze și aceste modificări.

Utilizarea translatarei NAT pentru ascunderea informațiilor despre rețeaua LAN

După cum puteți vedea, translatarea NAT poate fi folosită și pentru a ascunde informațiile despre rețeaua internă. Deoarece adresa IP efectivă a clientului nu este utilizată niciodată în Internet, devine dificil, dacă nu chiar imposibil, pentru cineva din rețeaua externă să o descopere.

Există însă o excepție. Unele aplicații încapsulează adresele sursă sau destinație în zona de informații utile a pachetului. Un exemplu semnificativ în acest sens este protocolul ICMP (Internet Control Message Protocol). Majoritatea pachetelor ICMP, cum ar fi Destination Unreachable (Destinație inaccesibilă) și Parameter Problem (Problemă legată de parametru), includ, ca parte a zonei de informații utile, pachetul IP original pentru care raportează o eroare. Pentru ca serverul NAT să opereze normal, trebuie să fie proiectat să cunoască această problemă astfel încât să poată modifica aceste tipuri de pachete. În primul rând, trebuie să fie capabil să modifice informațiile IP din antetul unui pachet IP care transportă mesajul ICMP. În al doilea rând, va trebui să modifice informațiile IP memorate în pachetul IP original și care sunt acum încapsulate de pachetul ICMP.

Atunci când evaluați produse care folosesc tehnologia NAT, citiți cu atenție documentația pentru a fi sigur că suportă serviciile de care aveți nevoie pentru rețeaua dumneavoastră.

Utilizarea translatarei NAT pentru creșterea spațiului de adrese din rețeaua LAN

Un alt avantaj al translatarei NAT este acela că vă permite să creșteți foarte mult spațiul de adrese din rețeaua internă. Înainte de dezvoltarea tehnologiei NAT, era necesar ca fiecare gazdă conectată la Internet să aibă propria adresă IP unică. Dacă două rețele care folosesc spații identice de adrese ar fi fost conectate la Internet, nu ar fi existat nici o metodă de a decide cum să fie rutate pachetele. Gândiți-vă ce s-ar întâmpla dacă mai multe case de pe strada dumneavoastră ar avea același număr. Cum ar putea poștașul să distribuie o scrisoare?

Folosind translatarea NAT, beneficiați de avantajul unor domenii de adrese stabilite de organizația IANA (Internet Assigned Number Authority). În loc să fiți obligat să vă descurcați cu o adresă de clasă C, cu numai 256 de adrese posibile, puteți folosi unul dintre domeniile de adrese rezervate. Desigur, oricine poate utiliza același domeniu de adrese ales de dumneavoastră. Ideea este că la trecerea în Internet, NAT va translata adresele dumneavoastră de rețea private în adrese valide. Dacă folosiți translatarea NAT de bază, va trebui să stabiliți pentru utilizare un domeniu valid de adrese. Dacă folosiți translatarea NATP, puteți să stabiliți mai puține adrese, deoarece poate fi variată valoarea numărului de port.

Unul dintre elementele importante care a stat la baza următoarei versiuni a protocolului Internet, IPv6, a fost convingerea că domeniul de adrese IPv4 va deveni rapid suprasaturat. NAT reduce această urgență, deoarece nici o rețea nu mai trebuie să aibă o adresă IP unică pentru fiecare gazdă proprie. În ultimii câțiva ani, mai multe organizații educaționale care au fost conectate la Internet încă din primii ani de utilizare a acestei rețele (și care foloseau domenii imense de adrese de clasă A) și-au reconfigurat rețelele proprii pentru a utiliza un domeniu privat de adrese. Astfel, adresele de clasă A au putut fi returnate pentru reutilizare în alte organizații. Cu toate că IPv6 este, fără nici o îndoială, viitorul rețelei Internet, pe termen scurt, NAT ameliorează urgența crizei de adrese.

Vezi și

➤ *IPv6 reprezintă viitorul dumneavoastră. Pentru mai multe informații despre acest protocol IP din generația următoare, vezi capitolul 21, „Firewall-uri și mai mult decât atât”, la pagina 306.*

Ce este vectorizarea adreselor?

Funcția denumită *vectorizarea adreselor* este foarte asemănătoare cu NAT.

Să presupunem că aveți un sit Web popular care primește un număr mare de vizite în fiecare zi. Pentru a satisface aceste cereri, ați putea achiziționa un server puternic, cu mai multe unități centrale de prelucrare și subsisteme de discuri RAID care suportă sarcina. Însă la un moment dat, se va ajunge într-un punct în care serverul, indiferent cât de mare este, începe să lucreze mai lent, iar timpul de răspuns va crește. Pentru un sit Internet mare, folosirea unui singur server este pur și simplu nefezabilă. O soluție ar putea fi utilizarea mai multor servere și atribuirea pentru fiecare server a unei adrese IP diferite și a unui nume DNS diferit. Însă această soluție nu este foarte practică. Folosind această metodă, clienții ar trebui să știe mai multe nume de gazde pentru a accesa situl dumneavoastră și ar trebui să încerce numele rând pe rând până când primesc un răspuns satisfăcător.

Vectorizarea adreselor vă permite să distribuiți încărcarea pe mai multe servere, toate acționând ca și cum ar fi același server care este adresat de un client. Nu este nevoie decât de un nume DNS și de o adresă IP. Tehnologia NAT permite translatarea mai multor adrese interne ale clienților într-o singură adresă IP externă validă. Vectorizarea adreselor funcționează similar, permițând unei singure adrese IP sosite să fie translataată în mai multe adrese IP în rețeaua dumneavoastră LAN. Astfel, puteți să adăugați mai multe servere pentru a echilibra încărcarea după cum doriți. Folosiți o aplicație intermediară care suportă vectorizarea adreselor pentru a decide ce server (de obicei cel mai puțin ocupat) va satisface cererea.

Vezi și

- Pentru a învăța cum să instalezi și să configurezi Microsoft Proxy Server, citești capitolul 18, „Microsoft Proxy Server”, la pagina 272.

Ecranarea și blocarea conținutului

Ecranarea accesului la Internet a devenit un subiect fierbinte în ultimii ani. Această capabilitate permite administratorului să desemneze câteva situri care vor fi blocate pentru utilizatorii din rețeaua locală. Unele produse vă permit să specificați siturile care trebuie blocate, în timp ce altele ecranează conținutul traficului de rețea și pot fi configurate pentru a bloca anumite cuvinte sau alte date. Dacă răspundeți de o rețea comercială, veți dori ca angajații dumneavoastră să își petreacă timpul producând ceva pentru companie și nu navigând în Web, în căutarea unor situri „interesante”.

Motivele pentru care puteți folosi tehnici de ecranare și blocare nu se limitează la obligarea angajaților să lucreze în interesul companiei. Puteți întrebuința aceste tehnici și pentru a reduce răspunderile legale. De exemplu, dacă unul dintre angajații dumneavoastră descarcă materiale dubioase (cum ar fi cele pornografice sau informații de pe un sit orientat spre violență), ar putea să fie răspunzătoare compania dumneavoastră dacă angajatul arată materialele respective cuiva care le găsește jignitoare? Este mult mai ușor să preveniți decât să încercați să rezolvați lucrurile după ce s-a petrecut evenimentul nedorit. Ca urmare, în prezent, tehnicile de ecranare și blocare devin din ce în ce mai populare.

Deoarece un server intermediar este plasat între clientul și serverul unui serviciu de rețea, pot fi utilizate mai multe metode pentru ecranarea sau blocarea accesului la nivelul serverului intermediar:

- **Blocarea adreselor URL** – Puteți să specificați adresele URL care vor fi blocate (sau înregistrate în jurnale). Dezavantajul acestei metode este că adresele URL se schimbă frecvent în Internet. Mii de pagini sunt adăugate zilnic și este practic imposibil pentru un administrator ocupat să evalueze fiecare sit nou.
- **Blocarea categoriilor** – Această metodă vă permite să specificați o anumită categorie de informații care va fi blocată. De exemplu, siturile care conțin materiale despre sex sau violențe.
- **Conținut înglobat** – Unele aplicații software intermediare pot fi configurate să blocheze obiectele Java, controalele ActiveX și alte obiecte care ar putea fi înglobate într-un răspuns la o cerere Web. Aceste tipuri de obiecte pot fi folosite pentru a rula aplicații pe un calculator local și, din acest motiv, pot fi utilizate și de hackeri pentru a obține acces.

Software-ul de blocare a conținutului nu este perfect și nu ar trebui să reprezinte singurul dumneavoastră mijloc de împiedicare a anumitor tipuri de date să circule în rețeaua proprie. Cu toate că puteți să specificați o listă lungă de adrese URL pe care doriți să le blocați, un utilizator bine informat ar putea să treacă de aceste blocaje folosind adresa IP a sitului în cererea HTTP. Ca și cum asta nu ar fi destul de rău, adresele IP nu trebuie scrise numai în notație zecimală cu punct. O adresă IP este de fapt un număr format din 32 de biți, iar notația zecimală cu punct este o metodă convenabilă de scriere a acestui număr.

Majoritatea browserelor vor accepta o reprezentare zecimală a adresei de 32 de biți (de exemplu, o valoare de număr întreg pentru valoarea pe 32 de biți). De exemplu, să analizăm adresa 216.65.33.219. În reprezentare binară, aceasta ar trebui să apară astfel:

216 = 11011000

65 = 01000001

33 = 00100001

219 = 11011011

Concatenând într-un șir toți acești biți, obțineți, în reprezentare binară, 11011000010000010010000111011011. Converteți acest număr în sistemul zecimal și obțineți valoarea 3628147163. Astfel, pentru a accesa situl Web care folosește adresa 216.65.33.219, în majoritatea browserelor puteți folosi oricare dintre următoarele notații:

http://216.65.33.219

http://3628147163

Nu vă bazați pe software-ul de blocare ca singură metodă de apărare împotriva programelor de tip cal troian și a virusilor de calculator. Programele care filtrează aceste tipuri de aplicații operează prin căutarea unei „amprente” cunoscute. Ele nu pot garanta protecția împotriva amenințărilor noilor virusi până când software-ul de filtrare nu este actualizat de furnizor. De asemenea, sunt ușor de ascuns programe virus în mesaje de poștă electronică. Din aceste motive, instalați un program bun de ecranare (și eliminare) a virusilor pe toate calculatoarele din rețea și asigurați-vă că setul de reguli de securitate din situl dumneavoastră interzice utilizatorilor să aducă software de acasă (în special pe dischete).

Facilități de înregistrare în jurnal și de avertizare

O funcție de securitate importantă pe care o oferă serverele intermediare și care nu trebuie trecută cu vederea sau tratată cu ușurință este capacitatea de înregistrare în jurnal a informațiilor despre activitățile pe care le desfășoară. Unele pot fi configurate pentru a declanșa o alarmă (de exemplu, un mesaj e-mail pentru administrator sau un mesaj pop-up la consolă) pe baza unor condiții predeterminate.

Serverele intermediare de nivel aplicație sunt capabile în mod obișnuit să ofere mai multe informații pentru înregistrarea în jurnal decât intermediarele generale sau de nivel circuit. Aceasta se datorează faptului că intermediarul de nivel circuit nu ia decizii decât pe baza informațiilor de adresare (adresa IP, numărul de port), la fel ca un filtru de pachete. Intermediarele de nivel aplicație sunt scrise pentru anumite servicii sau protocoale și, astfel, sunt capabile să extragă o cantitate mai mare de informații pentru înregistrarea în jurnal, deoarece „înțeleg” serviciul sau protocolul.

Înregistrarea în jurnal este o componentă importantă a auditării oricărui sistem, server intermediar, server de fișiere sau chiar a unei stații de lucru obișnuite. În capitolul 8, „Tehnici de monitorizare și auditare a sistemelor de operare”, acest subiect este prezentat mai detaliat pentru sistemele de operare Windows NT și UNIX. În plus, nu uitați să citiți documentația care însoțește orice software intermediar pe care îl achiziționați. Experimentați opțiunile de înregistrare în jurnal, revedeți datele capturate, până vă familiarizați cu informațiile pe care le puteți obține în acest mod. Configurarea unui sistem sau a unei aplicații pentru înregistrarea în jurnal nu ar trebui considerată o funcție statică. Cu toate că

inițial ați putea configura serverul pentru a înregistra numai o cantitate mică de informații în timpul operațiilor obișnuite, atunci când bănuieți că rețeaua dumneavoastră este atacată, ar trebui să înțelegeți cum funcționează mecanismele de înregistrare în jurnal, astfel încât să puteți permite o înregistrare mai detaliată a informațiilor respective.

Considerații referitoare la client

Dacă doriți să oferiți acces transparent către serviciile de rețea folosind servere intermediare, va trebui să acționați în una dintre următoarele direcții:

- Modificați software-ul client existent astfel încât să lucreze cu serverul intermediar.
- Obțineți un software client nou, care poate fi configurat să folosească un server intermediar.

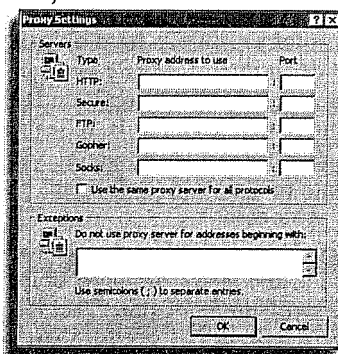
Dacă nici una dintre cele două variante nu este fezabilă, ați putea să luați în considerare utilizarea unui server intermediar clasic, de genul celor care se găsesc în pachetul TIS Internet Firewall Toolkit. Această soluție va implica instruirea utilizatorilor.

Majoritatea aplicațiilor noi au capacitatea de a folosi servere intermediare interne. De exemplu, Microsoft Internet Explorer poate fi configurat să utilizeze un server intermediar pentru unele sau pentru toate cererile de servicii de rețea.

1. În Internet Explorer, executați clic pe meniul Tools (Instrumente) și apoi selectați Internet Options (Opțiuni Internet). După afișarea ferestrei de proprietăți Internet Options, executați clic pe Connections (Conexiuni) și apoi pe butonul LAN Settings (Valori de configurare a rețelei LAN).
2. În caseta de dialog Local Area Network (LAN) Settings, selectați caseta de validare Use a Proxy Server (Folosește un server intermediar).
3. Introduceți adresa IP a serverului intermediar și portul care va fi folosit.
4. Utilizați caseta de validare Bypass proxy server for local addresses (Ocolește serverul intermediar pentru adresele locale), dacă acestui client îi este permis să contacteze direct servere din rețeaua locală.

FIGURA 7.4

Folosiți caseta de dialog Proxy Settings pentru a configura serverele intermediare pentru diferite servicii.



Dacă selectați caseta de validare Use the Same Proxy Server for All Protocols (Folosește același server intermediar pentru toate protocoalele), va fi disponibil numai primul câmp pentru a specifica adresa unui server intermediar și portul.

6. În caseta Exceptions (Excepții), listați toate serverele care doriți să fie contactate direct de clienți, prin ocolirea serverului intermediar. Separați gazdele folosind caracterul punct și virgulă.

7. Executați clic pe butonul OK după ce terminați.

În caseta de dialog Local Area Network (LAN) Settings, puteți să selectați și opțiunea ca serverul intermediar să se configureze automat cu ajutorul unui script pus la dispoziție de administrator. Pentru rețelele mari, această opțiune poate economisi timp.

Rezumat

Serverele intermediare reprezintă o componentă importantă a unui firewall. Lucrând la nivelul aplicației, aceste servere pot fi configurate pentru a permite sau a interzice selectiv caracteristici oferite de un serviciu sau un protocol de rețea. Capabilitatea lor de a executa înregistrări detaliate în jurnale și alertări este mai puternică decât cea oferită de filtrele de pachete, deoarece numeroase aplicații intermediare înțeleg foarte bine serviciul sau protocolul cu care lucrează. În capitolele următoare veți face cunoștință cu câteva soluții intermediare, între care se numără TIS Internet Firewall Toolkit, SQUID și Microsoft Proxy Server.

Tehnici de monitorizare și auditare a sistemelor de operare

- Auditare și fișiere jurnal
- UNIX
- Windows NT
- Fișiere jurnal specifice aplicațiilor
- Alte considerații

Auditare și fișiere jurnal

Siguranța pe care o oferă o arhitectură de firewall bine configurat nu ar trebui să fie o scuză pentru ca dumneavoastră să neglijați procedurile obișnuite privitoare la securitate. Chiar dacă aveți încredere în utilizatorii din rețeaua dumneavoastră locală – ceea ce nu este neapărat o idee bună – nu ar trebui să aveți încredere că firewall-ul vă protejează de toate relele posibile care pot să amenințe rețeaua dumneavoastră din exterior. Rețeaua Internet permite unui hacker răuvoitor să desfășoare un atac asupra rețelei LAN din aproape orice loc de pe glob. Există programe în Internet care automatizează procesul de căutare și penetrare a sistemelor și rețelelor vulnerabile. După configurarea și instalarea unui firewall, ar trebui să vă gândiți la acesta ca la o primă linie de apărare – nu ca la o soluție completă.

Ce este auditarea?

Atunci când discutați despre *auditare* (*auditing*), care este procesul de înregistrare a anumitor evenimente care au loc pe un calculator sau într-o rețea, este important să înțelegeți că numai prin această tehnică veți putea începe să detectați sursa unei compromiteri a rețelei. Dacă un răuvoitor infiltrat este capabil să distrugă date importante sau să blocheze un server important, veți afla foarte curând! Dar veți putea să determinați cauza? De exemplu, când are loc blocarea unui server, cum puteți fi sigur că evenimentul nu a fost provocat de o eroare de programare în sistemul de operare? Ar fi posibil ca blocarea să se datoreze unei

aplicații noi pe care tocmai ați instalat-o? Sau, și mai rău, persoana care a generat problema se găsește în interiorul sau în afara rețelei dumneavoastră?

Atât UNIX, cât și Windows NT au capabilități extinse de auditare. Însă nu puteți fi sigur că instalarea prestabilită a sistemului de operare va genera lista de evenimente auditate care vă vor fi cele mai utile. În acest capitol, vom discuta despre aceste aspecte și despre tipurile de informații pe care le pot dezvălui, precum și despre modul de configurare a funcțiilor de auditare oferite de aceste sisteme.

De ce este importantă auditarea?

Cea mai rea situație în care v-ați putea afla din punctul de vedere al securității rețelei este cea în care rețeaua dumneavoastră a fost infiltrată și habar nu aveți. Cu cât este mai mare perioada în care un hacker este capabil să reziste în sistemele atașate la rețeaua dumneavoastră, cu atât sunt mai mari pagubele pe care le poate provoca. Nu este vorba numai de paguba inițială – furt de informații confidențiale sau distrugerea unor date importante. Este vorba de timpul pe care îl acordați hackerului să „planteze” germeii unor viitoare aventuri în rețeaua dumneavoastră. Atâta vreme cât nu aveți habar că el este acolo, hackerul poate să înceapă înlocuirea unor programe importante de sistem cu versiuni modificate. El poate să creeze conturi de utilizator sau alte intrări secrete în rețea, astfel încât când descoperiți prima sa intruziune, rețeaua dumneavoastră este într-o asemenea harababură încât curățarea ei va fi un adevărat coșmar. Din acest motiv, pe lângă capabilitățile de auditare și înregistrare în jurnal ale firewall-ului, ar trebui să păstrați sub observație strictă fiecare sistem de operare instalat pe fiecare calculator din rețea. Instruiți-vă singur în legătură cu tehnicile care pot fi folosite și implementați-le în versiune completă. De asemenea, analizați des datele oferite de tehnicile de auditare – chiar foarte des!

Revedeți acele fișiere jurnal!

Nu are rost să folosiți tehnici extinse de auditare dacă nu stabiliți și un program de revedere regulată a fișierelor jurnal. Studiul fișierelor voluminoase utilizate pentru înregistrarea evenimentelor poate necesita foarte mult timp și este ușor să renunțați la această sarcină dacă aveți o zi ocupată. Însă există programe comerciale pe care le puteți folosi pentru a optimiza procesul. S-ar putea să nu fie nevoie să citiți fiecare eveniment din jurnalul de evenimente întreținut de sistemul Windows NT sau din fișierele mari care pot fi create prin utilizarea funcției syslog din UNIX.

Iată câteva lucruri importante pe care trebuie să le rețineți referitor la fișierele jurnal:

- Dacă este posibil să se pătrundă în sistemul dumneavoastră, cum puteți fi sigur că fișierele jurnal nu au fost compromise? Chiar puteți să aveți încredere în informațiile din fișierele jurnal proprii? Dacă intrusul în sistem a folosit un cont foarte privilegiat (cum este root), are și capabilitatea de a edita fișierele jurnal pentru a-și șterge urmele.
- Este ușor să deveniți superficial atunci când efectuați în mod repetat o procedură de rutină. Dacă aveți o sarcină zilnică de parcurgere a mai multor fișiere jurnal (care conțin informații foarte plictisitoare), cât de atent veți putea să fiți? Este posibil ca după câteva luni – sau ani – de citire a fișierelor, fără descoperiri importante, să omiteți o înregistrare importantă care dezvăluie o breșă de securitate?
- Fișierele jurnal pot deveni foarte mari. Este tentant să le ștergeți sau chiar să restricționați tipurile de evenimente înregistrate, astfel încât să nu vă faceți probleme referitoare la spațiul liber pe disc.

Certitudinea că informațiile înregistrate într-un fișier jurnal sunt corecte poate fi înșelătoare. Însă, în multe cazuri, acelea sunt toate datele de care dispuneți atunci când încercați să descoperiți sursa unei intruziuni. Dacă bugetul vă permite, puteți să rezolvați cea mai mare parte a acestei probleme prin plasarea fișierelor jurnal pe o unitate care folosește un suport ce nu poate fi scris decât o singură dată. Prețul unităților CD-ROM inscriptibile și al altor dispozitive cu o singură scriere a scăzut foarte mult în ultimii câțiva ani, astfel că nu ar trebui să fie prea dificil să justificați costul unei astfel de măsuri în fața conducerii a organizației. Această tehnică nu vă protejează de datele incorecte create de programele care au fost „sparte”. Dacă un intrus a reușit să înlocuiască fișierele importante de sistem care scriu în fișierele jurnal, aveți în continuare o mare problemă. Însă această tehnică împiedică intrusul să editeze un fișier jurnal pentru a-și șterge urmele pătrunderii în rețeaua dumneavoastră.

Securitatea este o sarcină importantă. Nu ar trebui să o lăsați în grija unei singure persoane. Pentru a depăși problema plictiselii care poate să apară la citirea fișierelor jurnal, puteți face mai multe lucruri. În primul rând, automatizați procesul folosind instrumente proiectate să consolideze sau să caute anumite informații în fișierele jurnal. În al doilea rând, atribuiți sarcina de revedere a acestor date mai multor persoane. Lăsați-i să efectueze această activitate o dată la câteva zile, astfel încât factorul plictisală să nu mai fie la fel de pregnant. Desigur, dumneavoastră, ca administrator, ar trebui să verificați frecvent procesul de auditare și revedere. Dacă există o singură persoană responsabilă pentru revederea informațiilor importante privitoare la securitate, această situație este ea însăși o potențială problemă de securitate. Este mai bine să aveți încredere în două sau mai multe persoane decât în una singură.

Este mai bine să produceți fișiere jurnal mari, care conțin o gamă largă de evenimente, decât să selectați numai câteva evenimente despre care credeți că ar putea reprezenta cu adevărat o problemă. De exemplu, în Windows NT puteți opta pentru auditarea operațiilor de conectare eșuate sau a celor reușite. Alegeți ambele variante! Cu toate că auditarea eșecurilor de conectare s-ar putea să nu producă un număr de înregistrări la fel de mare ca auditarea conectărilor reușite și, din acest motiv, să păstrați jurnalul de evenimente la o dimensiune mai mică, înregistrările cu conectările reușite pot fi un instrument mai valoros pentru a determina cum, când și de ce a fost spart sistemul de securitate al rețelei dumneavoastră. Numărul mare de conectări nereușite ar putea fi un semn că cineva încearcă să se infiltreze în rețea prin ghicirea parolilor și ar trebui să declanșeze o alarmă. Conectările reușite vă pot arăta când este folosit un cont de utilizator pentru a pătrunde în sistem în afara orelor de program sau de pe un calculator care nu ar trebui utilizat de acel cont.

Considerați datele din fișierele jurnal ca fiind la fel de valoroase ca cele mai importante date pe care le păstrați în rețeaua dumneavoastră. Nu ștergeți în mod regulat fișierele jurnal pentru a salva spațiu pe disc. Dacă nu folosiți suporturi cu o singură scriere, care pot fi stocate în siguranță pentru referințe ulterioare, faceți copii de siguranță ale fișierelor jurnal pe suporturi offline și păstrați-le o perioadă nedefinită. Atunci când apare o breșă de securitate, s-ar putea să descoperiți că s-a datorat unui program de tip cal troian plasat în sistemul dumneavoastră în urmă cu mai multe luni, sau poate chiar cu un an în urmă. Este recomandat să păstrați fișierele jurnal astfel încât să poată fi analizate cu minuțiozitate după o perioadă de timp (dacă este nevoie).

Dacă v-ați îndeplinit sarcinile mai mulți ani fără a avea probleme majore de securitate, s-ar putea să respingeți aceste argumente referitoare la fișierele jurnal ca fiind o pierdere de resurse care ar putea fi folosite mult mai bine în altă parte în organizația dumneavoastră. Însă atunci când vă conectați rețeaua la Internet, nu o să mai fie nicidecum valabilă „vechea poveste”. Acesta nu este decât începutul unei revoluții în domeniul calculatoarelor și comunicațiilor, iar experiența trecută va păli în comparație cu tipurile de probleme care apar la orizont.

Componenta vizibilă a auditării: protejarea resurselor

Auditarea este numai o componentă a securității sistemului. Cealaltă componentă este protejarea resurselor. În timp ce prezentul capitol este concentrat pe partea de auditare a procesului de securitate, capitolul 6, „Utilizarea unei gazde bastion”, vă oferă o bună introducere în metodele de protejare a resurselor și a datelor valoroase din sistem utilizând mecanismele de protecție a resurselor disponibile în sistemele de operare UNIX și Windows. Dacă stabiliți drepturile și privilegiile utilizatorilor și protecțiile resurselor într-un mod sigur, este posibil să nu ajungeți să analizați în mijlocul nopții datele din fișierele jurnal în încercarea de a descoperi ce a fost greșit.

UNIX

UNIX era considerat cândva *sistemul* de operare portabil. Era o soluție pentru numeroasele sisteme de operare private care s-au înmulțit atunci când nu existau decât câteva companii mari producătoare de calculatoare – doar minicalculatoare și calculatoare mainframe. În prezent însă, există mai multe variante sau versiuni de sisteme UNIX disponibile pe piață și este, probabil, cel mai folosit sistem de operare pentru calculatoarele conectate la Internet în scop comercial. Vărul său mai mic, Linux, a acaparat până în acest moment fragmente mari de piață și, datorită asemănării cu UNIX, o parte dintre lucrurile discutate aici despre UNIX sunt valabile și pentru Linux. Deoarece au fost distribuite mai multe versiuni diferite de UNIX, ar trebui să verificați cu atenție sintaxa specifică pentru comenzile prezentate aici ca exemplu.

Folosirea utilitarului syslog

O facilități importantă de auditare oferită de sistemul UNIX este utilitarul syslog, care preia datele de intrare de la o diversitate de programe și utilitare și le stochează într-o locație centrală. Datorită flexibilității sale, poate fi un instrument valoros de auditare numai dacă sunteți instruit în modul în care este configurat și înțelegeți evenimentele care sunt înregistrate.

Demonul syslog (syslogd) ar trebui pornit la încărcarea sistemului. Această operație este sarcina unuia dintre fișierele rc. Sintaxa pentru pornirea demonului este următoarea:

```
/etc/syslog [-mN] [-ffilename] [-d]
```

Numele prestabilit al fișierului de configurare pentru syslog este /etc/syslog.conf. Puteți să specificați un alt fișier folosind opțiunea -f urmată de numele fișierului de

configurare pe care doriți să îl utilizați. Poate fi o soluție utilă din două motive. În primul rând, specificând un nume de fișier care nu este standard, faceți ca încercarea unui hacker de a găsi și modifica fișierul să fie puțin mai dificilă. În al doilea rând, atunci când testați diferite configurații de înregistrare în jurnal, puteți să folosiți mai multe fișiere, astfel încât, dacă doriți să reveniți la o anumită configurație, nu trebuie decât să restatați utilitarul cu numele corect de fișier.

Opțiunea `-m` poate fi utilizată pentru a plasa mărci de timp în fișier. Opțiunea `-d` activează modul de depanare.

Pentru a configura modul de operare al demonului `syslogd`, ar trebui să consultați documentația care însoțește produsul firewall. Multe aplicații firewall vor folosi `syslogd` pentru înregistrarea în jurnal, iar furnizorul ar trebui să vă sugereze modul corespunzător de configurare a produsului respectiv.

Fișierul de configurare `syslog: syslog.conf`

Fișierul de configurare `syslog` este un fișier de text ASCII pe care îl puteți modifica folosind un editor de texte standard. Puteți să utilizați fișierul prestabilit `/etc/syslog.conf` sau, după cum a fost explicat în secțiunea anterioară, puteți utiliza un fișier diferit dacă porniți utilitarul specificând acel fișier ca opțiune. Acest fișier conține câte o înregistrare pentru fiecare tip de mesaj pe care doriți să îl înregistreze programul. Fiecare înregistrare se compune din două părți:

- Un selector care definește tipul de eveniment care trebuie înregistrat – sursa și gravitatea (severitatea) evenimentului.
- O acțiune care definește ce ar trebui să facă demonul `syslog` la producerea evenimentului.

Partea de selector din înregistrare este formată la rândul ei din două zone de informații, separate de un punct. Prima parte a selectorului este numele funcției de sistem care a generat mesajul de eveniment. A doua parte indică nivelul de severitate al mesajului. Pe o singură linie pot fi plasați mai mulți selectori, însă ei trebuie separați prin caractere punct și virgulă (`;`).

De unde prela utilitarul `syslog` mesajele?

Demonul `syslog` rulează ca proces în fundal, ascultă mesajele și decide pentru care dintre ele să acționeze pe baza regulilor stabilite în fișierul de configurare. De unde provin aceste mesaje? Din trei surse. În primul rând, există un soclu denumit `/dev/log` care recepționează mesaje de la procesele care rulează numai pe calculatorul local. În al doilea rând, există un dispozitiv `/dev/klog` care preia mesajele de la nucleul UNIX. În al treilea rând, portul UDP 514 recepționează mesaje de la alte calculatoare din rețea.

Tabelul 8.1 prezintă lista cu diferitele utilitare (facilități) din sistemul UNIX care pot fi utilizate în selector. Tabelul 8.2 listează nivelurile de severitate pe care le puteți specifica.

Tabelul 8.1 Nume de utilitare folosite în fișierul de configurare `syslog`

Utilitar	Descriere
user	Generat de aplicațiile utilizator
kern	Mesaje de nucleu
mail	Mesaje de sistem de poștă electronică

Utilitar	Descriere
daemon	Demoni de sistem
auth	Fișier de autorizare (de exemplu, login)
lpr	Sistemul de derulare a imprimantei de linie
news	USENET
uucp	UUCP (în prezent nu este implementat)
cron	Utilitarele cron și at
local0-7	Rezervat pentru utilizare locală
mark	Mesaje de tip marcă de timp
*	Toate cele precedente, exceptând mark

Tabelul 8.2 Niveluri de severitate folosite în fișierul `syslog.conf`

Niveluri de severitate	Descriere
emerg	Stare de panică. Ceva care se difuzează în mod obișnuit tuturor utilizatorilor.
alert	O situație care necesită atenție imediată.
crit	Avertismente despre situațiile critice.
err	Alte erori care nu justifică emerg, alert sau crit.
warning	Mesaje de avertizare.
notice	Situații care cer atenție, dar nu la fel de importante ca un avertisment sau altă eroare. Nu este în mod necesar o stare de eroare.
info	Mesaje informaționale.
debug	Mesaje generate de programe care rulează într-un mod de depanare.
none	Anulează mesajele pentru această intrare.

Crearea zonei de selector din înregistrare este o operație simplă. Nu trebuie decât să combinați una dintre facilitățile listate în tabelul 8.1 cu unul dintre nivelurile de severitate listate în tabelul 8.2. Pentru a le separa, folosiți un punct:

```
kernel.alert
auth.warning
mail.notice
lpr.crit
```

Această zonă de acțiune din înregistrare comunică demonului ce să facă atunci când recepționează un mesaj care corespunde criteriilor stabilite de zona de selector a înregistrării.

Pentru a termina înregistrarea, trebuie să specificați o acțiune care trebuie efectuată. Pentru a separa zona de selector de zona de acțiune a înregistrării sunt folosite unul sau mai multe caractere spațiu. Între tipurile de acțiuni care pot fi efectuate de syslog se numără următoarele:

- Scrie mesajul de eveniment într-un fișier jurnal (pe multe sisteme, /var/adm/messages).
- Trimite mesajul de eveniment unui alt calculator (prin portul UDP 514).
- Trimite mesajul de eveniment la dispozitivul consolă (/dev/console).
- Trimite mesajul de eveniment la un utilizator conectat la sistem.

Puteți să dați comanda syslog pentru a executa mai multe acțiuni pentru un anumit eveniment. De exemplu:

```
*.err;auth.notice           /dev/console
*.err;auth.notice;daemon.info /var/adm/messages
```

Pe prima linie a acestui exemplu, toate evenimentele cu nivelul de severitate err sunt scrise la dispozitivul consolă. Același lucru se petrece pentru evenimentele semnificative care au legătură cu autorizarea utilizatorului. Pe linia următoare, ambele tipuri de evenimente sunt trimise și în fișierul de mesaje. Trimițând mesajul la dispozitivul consolă (sau poate la un utilizator conectat la sistem), este de presupus că i se va da imediat atenție. Prin înregistrarea evenimentului în fișierul jurnal de mesaje, acesta poate fi revăzut după o perioadă de timp.

Observați în acest exemplu că sunt utilizate mai multe spații pentru a separa selectorul de zona de acțiune a înregistrării. Aceasta face ca fișierul să fie mai ușor de citit și întreținut, pentru că puteți vedea ambele porțiuni ale înregistrării. De ce este lizibilitatea atât de importantă? Deoarece, pe lângă revederea fișierelor jurnal, ar trebui să revedeți periodic și fișierul de configurare syslog pentru a fi sigur că nu a fost modificat de un intrus! De asemenea, puteți plasa comentarii în fișier adăugând un caracter # la început de linie. Dacă folosiți tehnici bune de formatare și comentarii care să vă ajute să înțelegeți de ce au fost plasate în fișier anumite înregistrări, sarcina de revedere a fișierului va fi mai ușoară. Anexa B, „Alte instrumente de securitate pe care le puteți folosi”, conține informații despre programe de securitate, cum ar fi Tripwire, pe care le puteți utiliza pentru a vă ajuta să verificați integritatea fișierelor sistem.

Atunci când utilizați un calculator gazdă UNIX ca parte a unui firewall, ar trebui să luați în considerare capabilitatea utilitarului syslog de a trimite mesaje unui alt calculator. De ce? Pentru că oricând este posibil ca gazda firewall-ului să fie compromisă de un intrus. Dacă un hacker a reușit să intre în sistem, poate fi capabil să editeze, să modifice sau chiar să ștergă fișierul jurnal de mesaje folosit de dumneavoastră. Trimițând mesaje altui sistem, crește puțin nivelul de securitate, deoarece hackerul va trebui să încerce să intre și în al doilea sistem pentru a ataca fișierul jurnal.

În funcție de importanța pe care o acordați securității în situl dumneavoastră, puteți dedica un singur calculator pentru a fi folosit ca legătură pentru mesajele syslog de pe alte sisteme. Prin întărirea acestui sistem – ștergerea conturilor de utilizator, dezactivarea serviciilor care nu mai sunt necesare și utilizarea unor protecții bune pentru fișiere – puteți face foarte dificilă pentru oricine încercarea de a perturba această evidență de auditare. Atunci când configurați soluții de securitate de acest gen, nu uitați că vă protejați de posibile atacuri atât din interiorul, cât și din exteriorul rețelei dumneavoastră.

Formatul de trimitere a mesajelor către alt calculator este următorul:

```
kern.*;ath.* @yoko.karma.com
```

Utilizarea unui fișier jurnal pentru mesaje este o idee bună, indiferent de celelalte acțiuni pe care le efectuați. Nu uitați că fișierele jurnal de dimensiuni mari pot fi mutate la intervale regulate de timp pe suporturi de stocare offline, astfel încât să nu ocupe foarte mult spațiu pe sistemul care rulează. În exemplele precedente, a fost utilizat fișierul standard /var/adm/messages. Puteți folosi acest fișier sau orice alt fișier pentru a păstra toate mesajele sau puteți folosi fișiere jurnal separate pentru tipuri diferite de evenimente. Utilizând mai multe fișiere jurnal, puteți face mai ușoară împărțirea sarcinilor de revedere a fișierelor între mai multe persoane care sunt capabile să înțeleagă mesajele înregistrate. De exemplu, administratorul de poștă electronică poate fi cea mai indicată persoană pentru revederea mesajelor despre sistemul de poștă electronică. Administratorul de sistem poate dori să revadă personal mesajele care au legătură cu nucleul UNIX. Utilizarea mai multor fișiere jurnal ușurează și scrierea de fișiere script care pot fi folosite pentru a vă ajuta în procesul de trecere în revistă a înregistrărilor.

Atunci când creați mai multe fișiere jurnal pentru a vă ajuta să organizați pe categorii mesajele înregistrate, rețineți că unele versiuni de UNIX limitează numărul de fișiere jurnal care pot fi deschise de demonul syslog. În unele cazuri, pot fi maxim 16 fișiere. Verificați documentația!

Diverse fișiere jurnal din sistemul UNIX

Demonul syslog nu este singura metodă utilizată pentru a produce fișiere jurnal pe un sistem UNIX. Deoarece UNIX are un trecut revoluționar în care diferiți autori sau producători au contribuit, în timp, cu noi componente, veți descoperi că există numeroase fișiere jurnal generate de diferite utilitare și care pot fi utile pentru revederea înregistrărilor.

usr/adm/wtmp, /etc/utmp și lastlog

Aceste trei fișiere binare țin evidența utilizatorilor din sistem. Fișierul etc/utmp afișează utilizatorii conectați curent la sistem, în timp ce usr/adm/wtmp este un fișier istoric, în care sunt înregistrate conectările la sistem, ieșirile din sistem și alte informații, cum ar fi momentul în care a fost oprit sistemul.

Fișierul /etc/utmp este menționat aici nu datorită utilității sale în probleme legate de securitate, ci din motivul exact opus. Conținutul acestui fișier se schimbă continuu pe măsură ce utilizatorii se conectează la sistem și ies din sistem. Problema principală a acestui fișier este că, în general, poate fi scris de orice utilizator pe cele mai multe implementări UNIX. Desigur, aceasta înseamnă că un intrus în sistem poate edita acest fișier pentru a șterge intrarea pentru conectarea sa curentă. Conținutul acestui fișier este folosit ca intrare pentru comanda who (și, de asemenea, pentru comenzile rwho și finger), astfel încât este bine să nu uitați că această comandă nu este neapărat o metodă foarte bună de determinare exactă a utilizatorilor conectați în sistem.

Fișierul usr/adm/wtmp nu șterge înregistrările atunci când un utilizator iese din sistem, ci păstrează o evidență de auditare a conectărilor și ieșirilor din sistem. Deoarece fișierul este scris continuu, iar înregistrările nu sunt șterse, este foarte indicat să fie salvat pe un suport care poate fi scris o singură dată. Procedând astfel, puteți preveni editarea (sau înlocuirea) acestui fișier de către un hacker. Pentru a obține informații din acest fișier pot fi utilizate

mai multe comenzi. De exemplu, comanda `last` poate fi folosită pentru a afișa informațiile în ordinea inversă celei în care sunt înregistrate în fișier, astfel încât să le puteți vedea începând cu cele mai recente.

Atunci când vă conectați într-un sistem UNIX, programul de conectare la sistem folosește un fișier denumit `lastlog` pentru a determina ultima dată când a fost utilizat acest nume de utilizator pentru conectare. În majoritatea versiunilor de UNIX, aceste informații sunt afișate la conectare. În unele versiuni, programul de conectare în sistem afișează și încercările reușite sau nereușite de conectare. Cu toate că nu vă oferă prea multe informații, fișierul poate fi util pentru a vă trezi suspiciuni în cazul în care vi se pare că ceva nu arată cum trebuie. De exemplu, dacă sunteți singura persoană care trebuie să folosească un anumit cont și observați că a fost efectuată o conectare anterioară într-un weekend, știind foarte bine că nu dumneavoastră ați fost cel care a făcut conectarea, este cazul să începeți să căutați în alte fișiere jurnal pentru a determina dacă altcineva v-a folosit contul!

`/var/adm/sulog`

Comanda `su` permite unui utilizator să comute utilizatorii. Ce înseamnă acest lucru? În timp ce este conectat cu contul propriu, un utilizator poate să utilizeze această comandă pentru a se conecta din nou, folosind un alt nume de utilizator și o altă parolă. Utilizarea comenzii `su` este înregistrată în fișierul `/var/adm/sulog`, astfel încât puteți vedea aceste situații. Comanda `sudo` este utilizată într-un scop similar, însă pentru aceasta nu este nevoie de parolă.

Aceste comenzi au o utilizare validă. Puteți avea un utilizator administrator care trebuie să folosească temporar un nume diferit de utilizator pentru a obține acces într-un anumit sistem de fișiere, de exemplu. Însă și un hacker care a reușit să intre în sistemul dumneavoastră poate folosi această comandă. În orice caz, revedeți periodic fișierul pentru a determina dacă vreuna dintre aceste comenzi este utilizată necorespunzător.

`/var/adm/aculog`

Acest fișier este utilizat pentru a ține evidența utilizatorilor care se conectează la alte sisteme prin modem pe linie telefonică. De asemenea, este folosit de comenzile UUCP pentru înregistrarea activităților proprii, chiar dacă în prezent UUCP nu mai este utilizat la fel de mult și a fost înlocuit de utilitare mai bune. Fișierul înregistrează utilizatorul care a efectuat apelul, numărul de telefon apelat și dacă apelul a fost reușit.

Capabilitățile de conectare pe linie telefonică către exterior și către interior sunt implementate cel mai bine de pe un calculator gazdă securizat care se găsește în zona DMZ sau poate pe un sistem care nu este conectat la rețea. Nu uitați că permițând calculatoarelor din rețea să aibă modemi interne, înseamnă că nu prea vă interesează accesul în rețea, așa că de ce să vă mai chinuiți să instalați un firewall?

`/var/log/cron`

Pentru automatizarea proceselor pe un sistem UNIX este utilizat demonul `cron`. Acest demon vă permite să creați fișiere script care pot fi rulate la ore și date specificate, fără intervenția utilizatorului. Cu toate că majoritatea implementărilor moderne ale demonului

folosesc facilitatea `syslog`, există și un fișier jurnal pentru acest demon, și anume `/var/log/cron`. Hackerii care sunt capabili să manipuleze fișierul de configurare al demonului `cron` pot să programeze rularea unui proces pe care îl pot folosi ulterior pentru a obține acces la sistem sau pentru a obține privilegii superioare. Revedeți regulat atât fișierul de configurare `cron`, cât și fișierul `log`. Și mai bine este să configurați demonul `syslog` să se ocupe de această auditare.

Comanda `ps`

Cu toate că nu folosește un fișier jurnal, comanda `ps` poate fi la fel de utilă ca un fișier jurnal atunci când investigați o posibilă breșă de securitate. În locul datelor din fișierele jurnal, comanda `ps` folosește tabelul de procese din nucleul UNIX și afișează informații despre procesele curente. Dacă un intrus a reușit să intre în sistemul dumneavoastră și a pornit un proces în fundal, puteți folosi această comandă pentru a-l căuta. Deoarece informațiile provin de la nucleu și nu de la un fișier jurnal, există puține șanse să nu fie corecte. În funcție de varianta de UNIX, comanda `ps` vă oferă următoarele informații:

- Identificatorul de proces
- Numele de utilizator
- TTY (terminalul folosit de utilizator)
- Ora începerii execuției
- Comanda executată curent
- Procentul de utilizare a unității centrale de prelucrare
- Procentul de utilizare a memoriei
- Ora când a fost pornit procesul

Când am discutat despre comanda `/etc/utmp`, am arătat că poate fi modificată de un hacker bine informat. Astfel, folosind această comandă și comparând rezultatele obținute cu conținutul fișierului amintit, puteți să identificați procese suspecte care justifică investigații ulterioare. De asemenea, căutați procesele care rulează de mai mult timp decât perioada normală, la o oră la care nu ar trebui să ruleze sau sunt lansate în execuție de un utilizator care nu ar trebui să execute o astfel de comandă.

Windows NT

Sistemul de operare Windows NT vă permite să auditați un număr mare de evenimente. Așa cum pe un sistem UNIX trebuie să configurați prima dată demonul `syslog` pentru a defini evenimentele care vor fi interceptate, și în Windows trebuie să stabiliți evenimentele care vor fi auditate.

Însă, spre deosebire de UNIX, nu trebuie să folosiți decât un singur utilitar – Event Viewer – pentru a vizualiza mesajele create. Un avertisment este că acest utilitar nu lucrează decât pentru sistemul de operare. Există unele aplicații, cum ar fi Internet Information Server, care actualizează și fișiere jurnal, pe lângă scrierea în fișierele Event Log. Există și aplicații de la alți producători care pot efectua fie una dintre cele două activități de auditare, fie ambele activități, în funcție de modul în care au fost programate.

Configurarea evenimentelor de auditare

În timp ce instrumentul administrativ Event Viewer este folosit pentru a analiza evenimentele auditate de sistemul Windows NT Server, există și utilitare care pot fi folosite pentru configurarea evenimentelor care vor fi auditate. Cele trei utilitare pe care le puteți folosi sunt următoarele:

- User Manager (sau User Manager for Domains într-un mediu în care au fost definite domenii)
- utilitarul Windows NT Explorer
- foaia de proprietăți (Properties Sheet) a unei imprimante

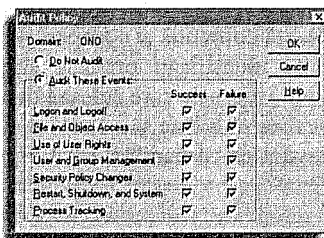
Primul utilitar pe care îl veți analiza este User Manager. Acest instrument de gestionare a sistemului, care se găsește în dosarul Administrative Tools (Instrumente administrative), este utilizat pentru a defini politica de auditare pentru server și pentru gestionarea conturilor de utilizator și a relațiilor de încredere pentru domeniu.

Selectarea evenimentelor pentru auditare utilizând User Manager Administrative Tool

1. Executați clic pe Start, Programs, Administrative Tools, și apoi selectați User Manager.
2. În meniul Policies (Politici), executați clic pe opțiunea Audit (Auditare). Pe ecran este afișată caseta de dialog Audit Policy (Politica de auditare) (vezi figura 8.1).
3. Executați clic pe butonul radio Audit These Events (Auditează aceste evenimente).
4. Pentru fiecare eveniment care doriți să fie auditat, selectați fie caseta de validare Success, fie caseta Failure (Eșec), fie ambele casete.
5. După ce terminați selectarea evenimentelor, executați clic pe butonul OK.

FIGURA 8.1

Caseta de dialog Audit Policy din User Manager for Domains este utilizată pentru configurarea evenimentelor care vor fi auditate.



Pentru fiecare tip de eveniment listat în caseta de dialog Audit Policy (vezi figura 8.1), puteți opta pentru auditarea evenimentelor încheiate cu succes și a evenimentelor nereușite. Un eveniment încheiat cu succes este cel în care accesul, cum ar fi conectarea la sistem a unui utilizator, a reușit. Un eveniment nereușit este opusul acestuia.

De exemplu, dacă nu doriți să știți decât momentul în care utilizatorii încearcă să se conecteze, dar eșuează din cauza unei parole incorecte sau din alt motiv, selectați caseta de validare Failure corespunzătoare acestui eveniment. De asemenea, puteți să optați pentru auditarea ambelor tipuri de evenimente, atât reușite, cât și nereușite.

Tabelul 8.3 oferă o scurtă explicație a fiecăruia dintre evenimentele pe care le puteți audita.

Tabelul 8.3 Evenimentele care pot fi auditate și pe care le puteți configura folosind instrumentul User Manager

Eveniment	Descriere
Logon and Logoff (Conectare la sistem și ieșire din sistem)	Ține evidența utilizatorilor care se conectează la sistem. De asemenea, ține evidența conectărilor în rețea de pe sisteme situate la distanță.
File and Object Access (Acces la fișiere și obiecte)	Include accesul la fișiere și directoare, precum și trimiterea de lucrări de tipărire către imprimante. Această categorie presupune ca dumneavoastră să definiți suplimentar evenimentele pentru fișierul, directorul sau imprimanta care va fi auditată.
Use of User Rights (Folosirea drepturilor utilizatorului)	Înregistrează când folosește un utilizator drepturile pe care i le-ați acordat atunci când i-ați configurat contul folosind instrumentul User Manager for Domains.
User and Group Management (Gestionarea utilizatorilor și grupurilor)	Ține evidența modificărilor pentru conturile de grupuri. Din această categorie fac parte crearea, ștergerea și redenumirea grupurilor de utilizatori, ca și schimbarea parolelor.
Security Policy Changes (Schimbări în politica de securitate)	Ține evidența schimbărilor în drepturile utilizatorilor și în relațiile de încredere sau de auditare.
Restart, Shutdown and System (Restartare, Oprire sau Sistem)	Ține evidența opririlor sau restartărilor sistemului și a altor evenimente care au legătură cu securitatea sistemului. Această categorie mai include modificările în evenimentul de securitate log on the system.
Process Tracking (Urmărirea proceselor)	Înregistrează informații voluminoase despre procesele utilizatorilor, inclusiv orele la care sunt executate programele, accesările obiectelor și ieșirile din program.

Dezactivarea auditării evenimentelor

În figura 8.1 puteți dezactiva auditarea tuturor evenimentelor care pot fi configurate cu ajutorul instrumentului User Manager, dacă executați clic pe butonul radio Do Not Audit (Nu audita). Dacă doriți să dezactivați auditarea doar pentru o scurtă perioadă de timp, folosiți acest buton. Utilizând butonul, evenimentele pe care le-ați selectat deja cu ajutorul casetelor de validare Success și/sau Failure rămân selectate. Dacă mai târziu decideți să reactivați auditarea, nu mai trebuie să vă amintiți ce evenimente ați avut selectate anterior. Nu trebuie decât să executați clic din nou pe butonul Audit These Events.

Dintre evenimentele prezentate în tabelul 8.1, ultimul, Process Tracking (Urmărirea proceselor), produce cel mai mare număr de înregistrări de evenimente. Deși ați dori să activați toate tipurile de evenimente pe un server care a fost „întărit“ pentru a rezista în zona DMZ, dacă selectați acest tip de eveniment vă trebuie o cantitate uriașă de spațiu pe disc pentru fișierele jurnal. Este recomandat să activați opțiunea Process Tracking numai

când investigați o anumită amenințare de securitate și trebuie să aveți această cantitate de informații detaliate pentru a vă dirija investigația.

După ce ați selectat evenimentele care vor fi auditate, sistemul de operare începe să creeze înregistrări în fișierele Event Log (Jurnal de evenimente) pentru toate evenimentele listate în tabelul 8.3, exceptând tipul de eveniment File and Object Access (Acces la fișiere și obiecte). Dacă ați optat pentru auditarea acestui tip de eveniment, trebuie să definiți suplimentar tipurile de evenimente care vor fi auditate utilizând Windows NT Explorer (pentru obiectele fișiere și directoare) și Print Manager (pentru imprimante).

În primul rând, trebuie să decideți pentru ce directoare sau fișiere trebuie auditat accesul. În al doilea rând, trebuie să hotărâți ce tip de acces să fie auditat. În continuare, folosiți Windows NT Explorer pentru a localiza și activa auditarea.

În figura 8.1, caseta de dialog Audit Policy vă permite să configurați politica de auditare pentru întregul domeniu. Rețineți că sistemul de operare Windows NT Server poate fi instalat ca un server independent sau ca un controller de domeniu. Când îl folosiți ca server independent, politica de auditare pe care o definiți se aplică numai acelui server. Când definiți o politică de auditare pe un server NT care operează ca un controller de domeniu, stabiliți politica pentru întregul domeniu.

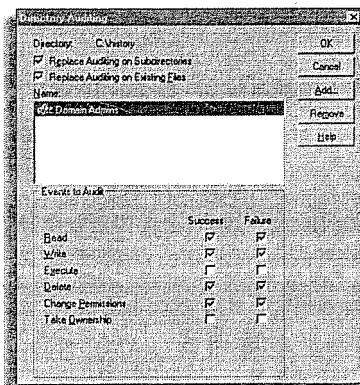
Din acest motiv (printre multe altele), ar fi imprudent să utilizați un controller de domeniu Windows NT ca gazdă bastion și apoi să optați pentru auditarea unui număr mare de evenimente. Dacă folosiți sistemul Windows NT Server ca o gazdă bastion, instalați sistemul de operare ca server independent, și nu ca un controller de domeniu.

Activarea auditării pentru un fișier sau un director

1. Executați clic pe Start, Programs, Windows NT Explorer.
2. Executați clic cu butonul drept al mouse-ului pe fișier sau pe director. O altă posibilitate este să executați clic pe numele fișierului sau directorului și să selectați opțiunea Properties (Proprietăți) din meniul File. Pe ecran este afișată pagina Properties Sheet pentru obiectul respectiv. Selectați eticheta Security din partea de sus a paginii Properties Sheet.

FIGURA 8.2

Selectați evenimentele care vor fi auditate pentru acest fișier sau director.



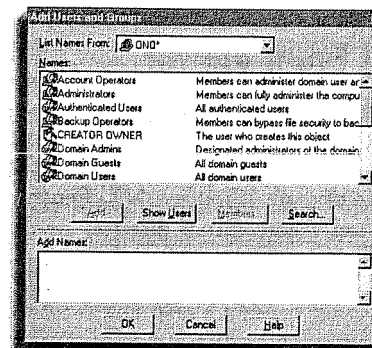
subdirectoare) dacă doriți să propagați aceste modificări de auditare în toate subdirectoarele plasate în directorul curent.

6. Selectați caseta de validare Replace Auditing on Existing Files (Înlocuiește auditarea pentru fișierele existente) dacă doriți să propagați aceste modificări de auditare în

toate fișierele existente în directorul curent (și în subdirectoare, dacă ați ales opțiunea respectivă).

FIGURA 8.3

Selectați utilizatorii și grupurile de utilizatori care vor fi auditate atunci când accesează fișierul sau directorul.



7. Executați clic pe butonul Add pentru a deschide caseta de dialog Add Users and Groups (Adaugă utilizatori și grupuri) (vezi figura 8.3).
8. Pentru a selecta un grup de utilizatori, executați clic pe numele grupului și apoi apăsați butonul Add. Grupul apare în fereastra Add Name, în partea de jos a casetei de dialog.

9. Pentru a selecta utilizatori individuali, executați clic pe un grup și apoi pe butonul Show Users (Afișează utilizatorii). Executați clic pe numele utilizatorului și apoi pe butonul Add. Utilizatorul este afișat în fereastra Add Name, în partea de jos a casetei de dialog.
10. O altă posibilitate de selectare este de a folosi butonul Search pentru căutarea unui utilizator sau a unui grup.
11. După ce ați terminat de selectat utilizatorii și/sau grupurile care vor fi auditate pentru evenimentele alese pentru fișierul sau directorul respectiv, executați clic pe butonul OK pentru a reveni în caseta de dialog Directory Auditing.
12. Executați clic pe butonul OK pentru a termina operația. Evenimentele de acces pe care le-ați selectat pentru fișier sau director sunt acum înregistrate în fișierele Event Log.

În figura 8.2 există șase tipuri de evenimente care pot fi selectate în vederea auditării pentru obiectele fișier sau director. Acestea sunt:

- Read (Citire)
- Write (Scriere)
- Execute (Execuție)
- Delete (Ștergere)
- Change Permission (Modificare permisiune)
- Take Ownership (Luare în proprietate)

Pentru a audita utilizarea imprimantei, folosiți o metodă foarte asemănătoare. Însă, în loc să utilizați Windows NT Explorer, puteți deschide pagina Properties Sheet a unei imprimante executând clic cu butonul drept al mouse-ului pe pictograma imprimantei, care se găsește în dosarul My Computer sau în dosarul Printers.

Evenimentele pe care le puteți audita pentru imprimante diferă însă de cele pentru fișiere și directoare:

- Print (Tipărire)
- Full Control (Control complet)
- Delete (Ștergere)

- Change Permission (Modificare permisiune)
- Take Ownership (Luare în proprietate)

Utilizarea instrumentului Event Viewer pentru revederea fișierelor jurnal

Event Viewer se găsește tot în dosarul Administrative Tools și este folosit pentru a analiza evenimentele auditate de sistemul de operare Windows NT. Pentru păstrarea înregistrărilor de evenimente sunt utilizate trei fișiere jurnal diferite, iar dumneavoastră puteți selecta ce fișier să examinați folosind acest utilitar. Cele trei fișiere jurnal sunt descrise în tabelul 8.4.

Tabelul 8.4 Utilizarea instrumentului Event Viewer pentru examinarea evenimentelor din fișierele jurnal

Fișier jurnal	Descriere
System (Sistem)	Evenimentele care au legătură cu operarea sistemului, cum ar fi pornirea, oprirea și defectările dispozitivelor.
Application (Aplicație)	Evenimentele înregistrate de aplicații.
Security (Securitate)	Evenimentele referitoare la problemele de securitate care au fost selectate pentru auditare.

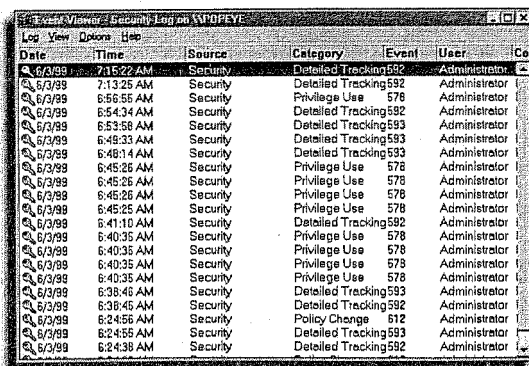
În timp ce fișierele jurnal System și Application pot fi utile pentru depanare, fișierul jurnal Security conține evenimentele pe care le-ați selectat pentru auditare.

Utilizarea instrumentului Event Viewer pentru examinarea evenimentelor auditate

1. Executați clic pe Start, Programs, Administrative Tools, și apoi selectați Event Viewer.
2. Selectați opțiunea Security din meniul Log (Jurnal) pentru a deschide fișierul jurnal Security (vezi figura 8.4).

FIGURA 8.4

Utilitarul Event Viewer afișează o listă de înregistrări care au rezultat în urma auditării.



Date	Time	Source	Category	Event	User	Co
6/3/99	7:15:22 AM	Security	Detailed Tracking	592	Administrator	
6/3/99	7:13:25 AM	Security	Detailed Tracking	592	Administrator	
6/3/99	6:56:55 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:54:34 AM	Security	Detailed Tracking	592	Administrator	
6/3/99	6:53:58 AM	Security	Detailed Tracking	593	Administrator	
6/3/99	6:49:33 AM	Security	Detailed Tracking	593	Administrator	
6/3/99	6:46:14 AM	Security	Detailed Tracking	593	Administrator	
6/3/99	6:45:26 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:45:26 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:45:26 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:45:26 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:41:10 AM	Security	Detailed Tracking	592	Administrator	
6/3/99	6:40:35 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:40:35 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:40:35 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:40:35 AM	Security	Privilege Use	578	Administrator	
6/3/99	6:38:46 AM	Security	Detailed Tracking	593	Administrator	
6/3/99	6:38:46 AM	Security	Detailed Tracking	592	Administrator	
6/3/99	6:24:56 AM	Security	Policy Change	612	Administrator	
6/3/99	6:24:56 AM	Security	Detailed Tracking	593	Administrator	
6/3/99	6:24:38 AM	Security	Detailed Tracking	592	Administrator	

3. Folosiți bara de derulare pentru a vă deplasa în fișier înainte și înapoi. Cele mai recente evenimente sunt afișate implicit la începutul fișierului.
4. Pentru a vedea detaliile asociate unui anumit eveniment, executați dublu clic pe eveniment în listing sau evidențiați evenimentul.

În figura 8.4, puteți vedea că prima linie a fiecărei înregistrări de eveniment începe cu o pictogramă. Aceste pictograme au o semnificație specială care ușurează operația de scanare prin fișier în căutarea evenimentelor serioase:

- **Semnul stop roșu** – Acest semn este ușor de văzut. Indică o eroare.
- **Punct de exclamare într-un cerc galben** – Acesta este un mesaj de avertizare.
- **Litera „I” într-un cerc albastru** – Acesta este un mesaj informațional.
- **Lacăt gri** – De interes special pentru probleme de securitate, acest semn indică un eveniment nereușit de autorizare.
- **Cheie aurie** – De asemenea, este de interes pentru probleme de securitate și indică un eveniment reușit de autorizare.

Gestionarea fișierelor jurnal de evenimente

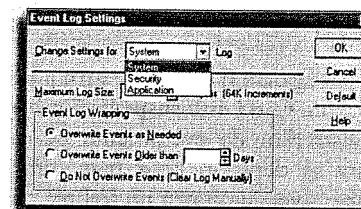
Folosind utilitarul Event Viewer, puteți să configurați modul în care sunt stocate evenimentele în fișiere, și puteți exporta datele într-un fișier care poate fi prelucrat ulterior cu ajutorul unei aplicații de calcul tabelar sau cu un alt program. Pentru a salva înregistrările de evenimente într-un fișier de text ASCII cu delimitator virgulă, selectați opțiunea Save As (Salvează ca) din meniul Log. În continuare, selectați opțiunea Comma Delimited Text (Text delimitat cu virgule) în câmpul Type (Tip). Când un fișier jurnal începe să crească mult în dimensiune, puteți folosi această metodă pentru a-l salva și apoi să goliți fișierul folosind opțiunea Clear All Events (Șterge toate evenimentele) din meniul Log.

Pentru a gestiona dimensiunea fișierului jurnal, utilizați opțiunea Settings (Valori de configurare) din meniul File.

Gestionarea fișierelor jurnal de evenimente

FIGURA 8.5

Puteți să controlați dimensiunea fiecărui fișier jurnal folosind caseta de dialog Event Log Settings.



1. Executați clic pe Log și apoi pe Settings. Pe ecran apare caseta de dialog Event Log Settings (vezi figura 8.5).
2. Folosiți câmpul Change Settings (Schimbă valori de configurare) pentru a selecta fișierul jurnal Security.

3. Folosiți câmpul Maximum Log Size (Dimensiunea maximă a jurnalului) pentru a stabili dimensiunea maximă la care poate ajunge fișierul jurnal.
4. Folosiți butoanele radio Event Log Wrapping pentru a controla dacă sunt suprascrise evenimentele mai vechi.
5. Executați clic pe OK pentru a termina.

Fișiere jurnal specifice aplicațiilor

Un producător de software care creează o aplicație poate opta pentru a implementa facilitatea de înregistrare în jurnal pentru produsul propriu. Dacă securitatea este importantă, ar trebui să luați în considerare acest aspect atunci când evaluați diverse produse. Dacă este nevoie de înregistrarea în jurnal, studiați amănunțit documentația pentru a afla modul în care este implementată această funcție. De exemplu, pentru o aplicație care rulează sub UNIX, programul creează și gestionează propriul fișier jurnal? Trimite portul UDP 514 mesaje la syslog? În cazul în care creează un fișier jurnal, puteți să precizați locația acestuia? Aceleași probleme sunt valabile și pentru o aplicație scrisă pentru a rula sub Windows NT: creează produsul un fișier jurnal propriu sau folosește facilitatea Event Logging? Abilitatea de a controla locația unui fișier jurnal specific unei aplicații este importantă, în special atunci când instalați aplicația pe o gazdă care va fi vulnerabilă. Direcționarea datelor de ieșire din fișierul jurnal către un dispozitiv cu o singură scriere vă poate ajuta să le protejați de eventualele modificări efectuate de un intrus.

Alte considerații

Atunci când am discutat pentru prima dată despre auditare, la începutul acestui capitol, am discutat și despre faptul că auditarea este partea din fundal a securității. Fișierele jurnal nu vă comunică decât ceea ce s-a întâmplat și nu fac nimic pentru a vă oferi un sistem securizat. Este important să folosiți caracteristicile de protejare a resurselor puse la dispoziție de sistemele de operare pentru a limita accesul la resursele importante, astfel încât în cazul în care cineva încearcă să intre în sistem fără permisiunea dumneavoastră, să fie nevoit să își folosească toate cunoștințele pentru a obține date sau pentru a periclita sistemul. Capitolul 6, „Utilizarea unei gazde bastion”, conține o discuție mai lungă despre protecțiile de resurse, așa cum sunt implementate de sistemele UNIX și Windows NT.

Rezumat

Auditarea este un instrument valoros care poate fi utilizat pentru a îmbunătăți securitatea fiecărui sistem din rețeaua dumneavoastră. Când este suspectată o breșă de securitate sau o intruziune în rețea, evidența înregistrărilor de evenimente pe care o puteți găsi în diferitele fișiere jurnal vă poate ajuta să depistați ce a fost compromis și, eventual, persoana care a efectuat operațiile respective. Auditarea nu trebuie considerată o operație de tip „configurează și uită”. Revederea periodică a fișierelor jurnal pentru a căuta evenimente neobișnuite ar trebui să fie ceva normal. Astfel, sunteți mult mai aproape de descoperirea unei intruziuni minore înainte ca hackerul să aibă timp să creeze mai multe pagube în rețeaua dumneavoastră.

Partea a II-a

Criptare și comunicații sigure în Internet

Capitolul 9 • Tehnologii de criptare	166
Capitolul 10 • Rețele virtuale private (VPN) și tuneluri	175
Capitolul 11 • Utilizarea programului PGP (Pretty Good Privacy) pentru criptare	188

Capitolul 9

Tehnologii de criptare

- Protejarea informațiilor importante
- Ce este criptarea?
- Aplicații practice pentru criptografie în Internet

Protejarea informațiilor importante

Utilizarea superautostrăzii informaționale (Information Superhighway), cum le place multora să numească rețeaua Internet, poate fi riscantă pentru transferul informațiilor valoroase sau importante. Deoarece majoritatea sistemelor prin care vor călători datele dumneavoastră în drumul lor către destinație nu sunt sub controlul dumneavoastră, există multe puncte din legătură în care pot fi interceptate datele. Pentru a face acest canal de comunicații sigur pentru transferuri comerciale, sunt utilizate tehnici de criptare care transformă datele obișnuite în *text cifrat (ciphertext)*. Aceasta înseamnă că este utilizat un algoritm matematic, împreună cu o cheie, pentru a executa o acțiune asupra datelor obișnuite, ceea ce produce un rezultat care pare să nu aibă sens. Cei care dețin cheia pot efectua procesul invers. Cei care nu dețin cheia nu pot înțelege datele criptate, desigur, mai puțin în cazul în care sunt criptografi experimentați, specializați în spargerea codurilor criptografice, și dispun de timp și resurse suficiente de calcul.

Acesta nu este singurul motiv pentru care poate fi folosită criptografia în Internet. Pentru a avea o imagine completă, iată care sunt cele trei funcții de bază pentru care este utilizată criptografia în Internet:

- Confidențialitatea
- Integritatea datelor
- Autentificarea

Este ușor să vă dați seama că scopul criptării datelor este de a le face să fie private. Numai expeditorul și destinatarul vor fi capabili să înțeleagă datele, astfel că este o comunicație privată. Însă cum puteți avea încredere în această metodă dacă nu sunteți sigur de unde provin cu adevărat datele? După ce sunteți sigur de expeditor, cum puteți fi sigur că datele nu au fost interceptate și modificate de o terță persoană? Utilizând tehnicile criptografice pentru a rezolva ultimele două probleme – autentificarea și integritatea datelor – creați o bază pentru comunicații sigure prin Internet.

În capitolul următor vom discuta o aplicație foarte practică a criptografiei, care poate fi utilizată pentru a rezolva toate cele trei probleme amintite – rețelele virtuale private

(VPN). Însă înainte de aceasta, în prezentul capitol vom trece în revistă rapid câteva dintre tehnicile fundamentale de criptare.

Ce este criptarea?

Criptarea este o metodă care poate fi utilizată pentru a ascunde conținutul unui mesaj de persoanele care nu trebuie să îl înțeleagă. În practică, majoritatea tehnicilor criptografice moderne se bazează pe formule matematice utilizate pentru a amesteca datele astfel încât să fie foarte dificil de înțeles de cineva care nu deține *cheia (key)*. Cheia este un șir numeric sau alfabetic de caractere, utilizat pentru criptarea sau descifrarea mesajului. Evident, cu cât cheia este mai mare, cu atât va fi mai dificil de descifrat un mesaj dacă nu cunoașteți cheia.

Există două tipuri fundamentale de criptare care au aplicații bune când sunt utilizate în Internet. Acestea sunt criptarea cu o singură cheie (simetrică) și criptarea cu chei publice (asimetrică).

Criptarea cu o singură cheie

Forma fundamentală de criptare este numită criptare cu o singură cheie. Această metodă folosește pentru criptarea datelor un algoritm matematic și o cheie unică. Aceeași cheie utilizată pentru criptare este utilizată și pentru decriptarea textului cifrat. Aceasta înseamnă că ambele părți implicate în comunicație trebuie să posede aceeași cheie și trebuie să o păstreze secretă. Dezvăluirea cheii ar putea permite oricui să citească textul.

Această formă de criptare mai este cunoscută și sub numele de *criptare simetrică (symmetric encryption)*, deoarece este utilizată o singură cheie pentru criptarea sau descifrarea datelor. Criptarea simetrică poate fi foarte rapidă și acesta este unul dintre avantajele utilizării ei. Chiar dacă o singură cheie face ușor de construit un algoritm foarte rapid de criptare, aceasta este și principala problemă a acestei tehnici. Înainte de începerea comunicației, una dintre părți trebuie să fie capabilă să trimită într-un mod securizat o copie a cheii către cealaltă parte. Pentru guverne, spioni și corporațiile mari, aceasta nu este o problemă atât de grea. Poate fi trimis un curier pentru livrarea în siguranță a unei chei secrete către cei care vor avea nevoie ulterior de cheie pentru comunicații criptate. Este evident că această tehnică nu va fi potrivită pentru o companie de afaceri care dorește să realizeze comunicații sigure cu mii (sau chiar mai mult) de clienți prin Internet. Este pur și simplu prea costisitor să fie trimis un curier la toți clienții.

Astfel, cu toate că tehnicile de criptare simetrică pot fi utilizate pentru a crea programe criptografice extrem de rapide și eficiente, lipsa unei metode sigure de transmitere a cheii pare să limiteze utilitatea acestui tip de criptare în Internet.

Iată câteva exemple de criptare simetrică:

- **DES** Metoda de criptare Data Encryption Standard a fost dezvoltată de firma IBM și Agenția Națională pentru Securitate (National Security Agency). DES utilizează o cheie de 56 de biți și operează cu blocuri de 64 de biți de text clar. Există și o versiune mai nouă, denumită 3DES, care utilizează trei chei diferite pentru a cripta datele de trei ori.

- **IDEA** Algoritmul IDEA (International Data Encryption Algorithm) folosește o cheie de 128 de biți, și din acest motiv, este mai rezistent la atacuri directe care încearcă să descifreze textul prin testarea fiecărei chei posibile.
- **Slipjack** Acest algoritm nou, clasificat ca secret, a fost dezvoltat de Agenția Națională pentru Securitate (National Security Agency) și folosește o cheie de 80 de biți.
- **Blowfish** Acesta este un algoritm de criptare simetrică și poate fi utilizat ca înlocuitor pentru DES și IDEA. Poate utiliza o cheie cu dimensiunea variind de la 32 la 448 de biți.

Criptare gratuită?

Deoarece nu este patentat, iar codul sursă este disponibil gratuit în Internet, algoritmul Blowfish (dezvoltat de Bruce Schneier) se răspândește rapid printre utilizatori. Pentru mai multe informații despre Blowfish, inclusiv o listă cu produsele care îl folosesc în mod curent, sau pentru descărcarea codului sursă, vizitați următorul sit Web:

www.counterpane.com/blowfish.html

Criptarea cu chei publice

Problema distribuirii cheilor este rezolvată prin folosirea criptografiei cu chei publice. Această metodă utilizează nu o singură cheie, ci două; din acest motiv, mai este numită criptografie asimetrică. O cheie este folosită pentru criptarea datelor, iar cealaltă cheie pentru decriptare. Între cele două chei există o relație matematică și împreună sunt cunoscute ca o pereche de chei. Utilizatorul păstrează o cheie secretă (cheia privată, sau personală) și „publică” cealaltă cheie (cheia publică), astfel încât oricine are nevoie de ea să o poată folosi. Atunci când doriți să trimiteți un mesaj criptat unei persoane care a generat o pereche de chei, criptați pur și simplu datele proprii cu cheia publică a persoanei respective. După ce mesajul a fost criptat, numai cheia personală a persoanei respective, care reprezintă secretul acesteia, poate fi folosită pentru descifrarea și citirea mesajului.

După cum puteți vedea, metoda de criptare cu chei publice rezolvă problema de a face datele imposibil de citit, precum și problema distribuției cheilor. Nu este nevoie ca o cheie publică să fie păstrată secretă. Mai mult, nici nu contează cine cunoaște cheia publică, deoarece poate fi folosită doar pentru a cripta datele, nu și pentru decriptare. De asemenea, această metodă conduce ea însăși la o utilizare universală. Dacă tuturor utilizatorilor din Internet li s-ar atribui o pereche de chei, iar cheile publice ar fi publicate, asemănător modului în care numerele de telefon sunt distribuite printr-o carte de telefoane, ar fi posibil ca aproape oricine să comunice în siguranță cu oricine altcineva.

Dezavantajul utilizării acestei metode de criptare este acela că, de obicei, nu este la fel de rapidă comparativ cu criptarea cu o singură cheie. Pentru fișierele de text mici și simple, viteza nu diferă foarte mult. Pentru fișierele mult mai mari, diferența poate fi semnificativă. Pentru o organizație de afaceri care așteaptă stabilirea unui canal sigur de comunicații, cum ar fi o rețea virtuală privată (VPN), cu un alt sit, viteza devine o necesitate.

poate fi calculată cheia personală folosind cheia publică?

Întotdeauna este posibil să fie învinsă orice tehnică criptografică, dacă există suficientă putere de calcul și suficient timp. Însă, din punct de vedere practic, dacă folosiți o cheie de dimensiune suficient de mare, ar fi foarte dificil pentru oricine să determine cheia dumneavoastră personală pornind numai de la cheia publică. Deoarece puterea de calcul

devine tot mai mare de la un an la altul, s-ar părea că dimensiunile cheilor și algoritmi utilizați în viitor se vor schimba pentru a se adapta acestor progrese tehnologice. Însă, în prezent, dacă folosiți o aplicație bună de criptare de la un furnizor de încredere, nu ar trebui să vă îngrijoreze prea mult faptul că cineva v-ar putea descoperi „secretul”.

Sisteme hibride

Tehnicile criptografice simetrice sunt rapide. Tehnicile criptografice cu chei publice sunt lente. Prin combinarea celor două metode într-un sistem hibrid este posibil să beneficiați de majoritatea avantajelor oferite de fiecare sistem în parte.

De exemplu, programul software de criptare Pretty Good Privacy (PGP) folosește și criptarea simetrică, și criptarea cu chei publice. Un mesaj este criptat inițial cu ajutorul unei chei speciale, generate aleator, care nu este valabilă decât pentru o utilizare – o cheie de sesiune. După ce mesajul este criptat folosind o tehnică simetrică (rapid), cheia de sesiune este criptată folosindu-se jumătatea publică a perechii de chei. Deoarece cheia de sesiune este mult mai scurtă decât mesajul utilizat pentru criptare, timpul necesar pentru criptarea acestei chei de sesiune cu cheia publică a utilizatorului este foarte mic.

Vezi și

- *Instalarea și configurarea programului Pretty Good Privacy (PGP) sunt prezentate în detaliu în capitolul 11, „Utilizarea programului PGP (Pretty Good Privacy) pentru criptare”, la pagina 188*

Atunci când destinatarul mesajului dorește să decodifice mesajul, folosește propria cheie secretă pentru decriptarea cheii de sesiune. Mesajul poate fi apoi descifrat rapid folosindu-se un algoritm simetric și cheia de sesiune.

Protocolul Secure Sockets Layer (SSL), dezvoltat de firma Netscape, este tot un hibrid care folosește criptarea simetrică și asimetrică și este prezentat detaliat chiar în acest capitol.

Aplicații practice pentru criptografie în Internet

Anterior în acest capitol, am menționat utilizarea programului PGP pentru criptarea mesajelor de poștă electronică. Însă, pentru a face mai eficientă folosirea criptării în Internet, va fi necesară stabilirea de standarde și servicii bazate pe aceste standarde care să poată fi încorporate în diverse aplicații, multe dintre ele fiind mai complexe decât sistemele simple de poștă electronică. Dacă fiecare furnizor de aplicații ar folosi un algoritm propriu pentru a produce aplicații sigure, s-ar ajunge la un set mare de aplicații sigure care nu ar putea comunica între ele. Între etapele importante care au fost parcurse până la metodele standard se numără folosirea semnăturilor digitale și a certificatelor digitale pentru autentificare, și utilizarea protocolului Secure Sockets Layer (SSL) pentru a permite schimburi sigure de date în Web.

Ce sunt semnăturile digitale?

Utilizarea criptografiei cu chei publice rezolvă problema trimiterii în siguranță a unui mesaj ce nu poate fi citit decât de destinatarul care deține cheia personală necesară pentru deblocarea mesajului. Această metodă rezolvă și problema distribuirii cheilor, deoarece

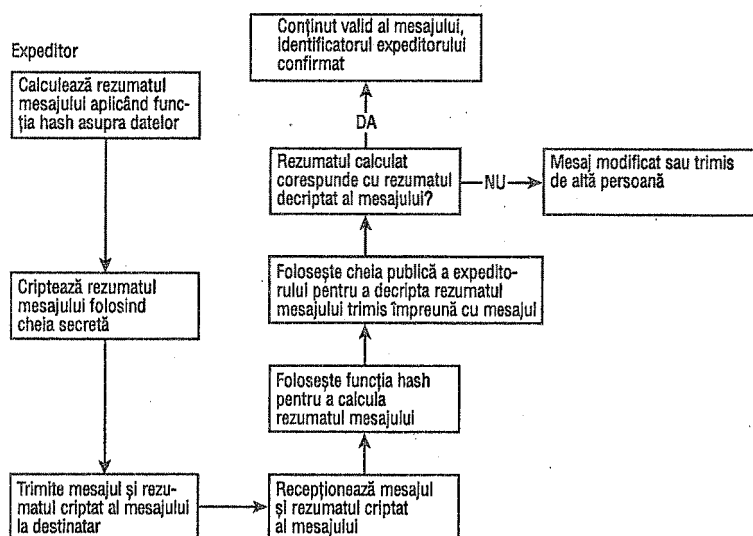
cunoașterea cheii publice nu permite descifrarea mesajului. Un lucru care nu este încă rezolvat este problema garantării la destinatar că expeditorul este cine spune că este. De exemplu, dacă ați recepționat un mesaj de poștă electronică de la Bill Gates, ați putea presupune că este vorba de o glumă făcută de cineva prin falsificarea unei adrese e-mail. Cum ați putea dovedi că: 1) Bill Gates a trimis într-adevăr mesajul și 2) mesajul este exact ceea ce a trimis Bill?

Soluția acestei probleme este o semnătură digitală. Să analizăm, de exemplu, ce s-ar întâmpla dacă ați fi folosit cheia dumneavoastră secretă pentru a cripta un mesaj, în loc să folosiți cheia publică a destinatarului. Deoarece numai dumneavoastră dețineți cheia secretă, cineva care poate să descifreze textul folosind cheia dumneavoastră publică ar ști că mesajul vă aparține. Desigur, după cum puteți vedea, aceasta înseamnă că oricine are acces la cheia dumneavoastră publică va fi capabil să descifreze mesajul. Amintiți-vă că perechile de chei publică/secretă operează în ambele direcții. Datele care sunt criptate cu o cheie pot fi decriptate numai cu cealaltă cheie din pereche.

Pentru a depăși această problemă, o semnătură digitală operează nu prin criptarea întregului mesaj, ci prin criptarea datelor produse de utilizarea unei funcții hash asupra mesajului. O funcție hash va produce un șir de date care de obicei este mult mai mic decât mesajul original, o valoare uzuală fiind 160 de biți. După cum este prezentat în figura 9.1, rezultatul unei funcții hash, denumit uneori *rezumat al mesajului* (*message digest*), este apoi criptat folosind cheia dumneavoastră secretă și trimis împreună cu mesajul. Dacă destinatarul poate decripta textul hash, poate să execute aceeași funcție hash asupra restului mesajului. Dacă valoarea hash calculată de destinatar pentru mesaj se potrivește cu textul hash criptat anterior cu ajutorul cheii secrete a expeditorului, se poate presupune că mesajul provine de la persoana respectivă și că a rămas intact și nemodificat. *Integritatea datelor* rămâne intactă. Orice modificare în mesaj va provoca recalcularea funcției hash și are ca rezultat un text hash diferit de cel produs de mesajul original.

FIGURA 9.1

Semnăturile digitale pot fi folosite pentru a garanta integritatea datelor și identitatea expeditorului.



După cum puteți vedea, această metodă semnifică faptul că pentru expeditor va fi foarte dificil să se decidă de un mesaj trimis folosindu-se semnătura sa digitală. Această tehnică se numește *nonrepudiare*, deoarece semnătura digitală poate fi aplicată numai de expeditorul original al mesajului, presupunând însă că acesta păstrează secretă cheia sa privată.

Un alt lucru care ar trebui să fie evident este că, atunci când folosiți o semnătură digitală, nu trebuie să criptați textul propriu-zis al mesajului. Puteți să faceți și acest lucru, însă nu acesta este scopul calculului pentru semnătura digitală. S-ar putea ca mesajul să nu conțină date importante, iar dumneavoastră să vreți doar să garantați autenticitatea expeditorului și integritatea mesajului. Valoarea hash poate fi calculată pentru mesaj indiferent dacă este sau nu criptat. Ideea este că, datorită folosirii aceleiași funcții hash la ambele capete ale comunicației, și pentru că expeditorul este singura persoană care păstrează cheia secretă folosită la crearea semnăturii, sursa comunicației poate fi verificată.

Certificate digitale

Certificatele digitale funcționează într-o manieră similară cu semnăturile digitale. Un certificat este un document care, în esență, spune că puteți „avea încredere” într-o anumită informație. Să presupunem că doriți să trimiteți un mesaj unei persoane folosind criptarea cu chei publice. La început trebuie să obțineți cheia publică a persoanei respective, astfel încât să puteți cripta mesajul. Însă, și aici este partea frumoasă, cum obțineți confirmarea că acea cheie publicată este într-adevăr cheia publică a destinatarului? Dacă nu ați comunicat încă securizat cu cineva și primiți o copie a cheii sale publice printr-un mesaj de poștă electronică sau de la un furnizor de astfel de lucruri din Internet, cum puteți fi sigur că este o cheie validă? S-ar putea să fie vorba de altcineva care vă trimite propria cheie publică, sperând să vă păcălească și să comuniceți cu el, dumneavoastră crezând că este altă persoană.

Un certificat digital poate fi folosit pentru a verifica faptul că o cheie publică aparține cu adevărat persoanei căreia credeți că îi aparține. Un certificat digital se bazează pe utilizarea unei terțe părți, care este cunoscută și de încredere. Certificatul va conține cheia publică, informații despre deținătorul cheii și, în final, o semnătură digitală pentru verificarea conținutului certificatului. Terța parte responsabilă pentru emiterea certificatului – denumită autoritate de certificare (Certificate Authority, sau CA) – trebuie să fie cineva cunoscut și în care aveți încredere. Compania Verisign este un exemplu de astfel de terț emitent de certificate. Deoarece aveți încredere în autoritatea de certificare și îi puteți verifica semnătura, puteți avea încredere în informațiile din certificat.

Nu este obligatoriu să vă bazați pe cineva din exterior pentru serviciile CA. Dacă necesitățile sunt interne, organizația dumneavoastră poate să configureze cu ușurință un server de certificare propriu, folosind un software disponibil pentru sistemele UNIX (ca program de completare) sau serverul de certificare livrat cu sistemul Windows 2000 Advanced Server. Folosind propria autoritate de certificare, veți fi nevoit să creați proceduri pentru emiterea și gestionarea certificatelor, însă va fi mult mai ieftin decât utilizarea serviciilor de la un furnizor extern.

Dacă cerințele dumneavoastră pentru certificate digitale includ schimbul de date cu alte organizații sau cu utilizatori din afara companiei, soluția este apelarea la un alt furnizor, cum ar fi Verisign.

Luați-vă propriul certificat digital

În Internet există câteva autorități de emitere a certificatelor care pot fi folosite pentru a obține un certificat digital sau pentru a căuta cheia publică a unei persoane care posedă așa ceva. Puteți să vizitați firma Verisign la următoarea adresă URL pentru a afla mai multe despre serviciul pe care îl oferă, care include testarea gratuită timp de 60 de zile:

www.verisign.com

Protocolul Secure Sockets Layer (SSL)

Piața pentru comerțul electronic, aflată în creștere în Internet, nu ar fi fost posibilă fără o tehnologie care să garanteze comunicații sigure. Pentru îndeplinirea acestei cerințe, firma Netscape a dezvoltat protocolul SSL (Secure Sockets Layer). SSL folosește tehnici criptografice pentru criptarea fluxului de date, pentru autentificări și pentru a garanta integritatea datelor transmise.

SSL este un protocol stratificat, format din alte două protocole: protocolul de înregistrare SSL și protocolul pentru dialogul de confirmare SSL. Procedurile dialogului de confirmare, pe care clientul și serverul le folosesc pentru a se autentifica reciproc și pentru a schimba informații despre chei, sunt executate de protocolul pentru dialogul de confirmare SSL. Protocolul de înregistrare SSL răspunde de formatarea datelor.

SSL 2.0 și SSL 3.0

Cea mai nouă versiune a protocolului SSL este 3.0. Această versiune completează versiunea 2.0 cu funcția de autentificare a unui client pe server.

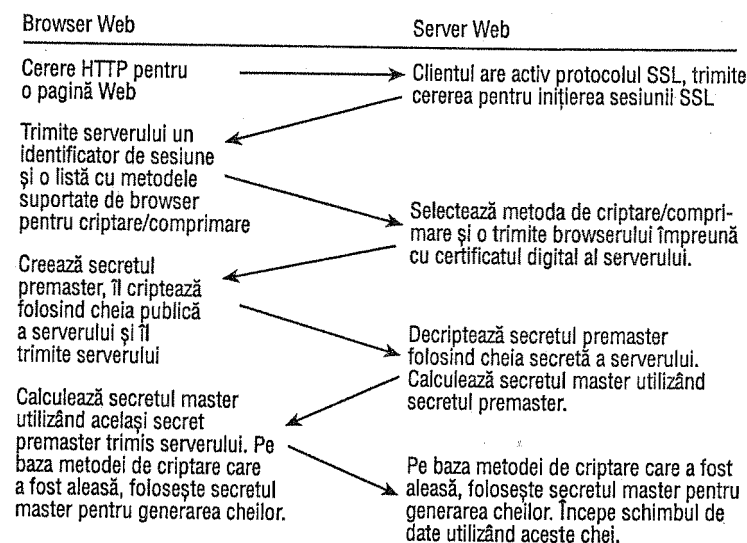
Procesul de confirmare (după cum este prezentat în figura 9.2) este următorul:

1. Un browser se conectează la o pagină către care se permite să folosească protocolul SSL. Serverul trimite o cerere de începere a unei sesiuni SSL către browserul client.
2. Dacă suportă protocolul SSL, browserul trimite un răspuns către server, răspuns care conține un identificator de sesiune și o listă cu algoritmi de criptare și metodele de comprimare suportate de browserul clientului. Acest prim mesaj mai include ora și data curente, precum și un set de date generate aleator.
3. Serverul selectează o metodă de criptare și comprimare și trimite un mesaj browserului, împreună cu identificatorul de sesiune și o serie de date generate aleator. Pentru a se autentifica în fața clientului, serverul mai trimite și propriul certificat digital.
4. Opțional, serverul ar putea să trimită clientului o cerere prin care să îi solicite acestuia trimiterea certificatului digital.
5. În funcție de tipul de cifru ales pentru sesiune, clientul creează un mesaj denumit *secret premaster*, criptează datele din mesaj folosind cheia publică a serverului și trimite mesajul către server.
6. Serverul decriptează datele secretului premaster folosind cheia sa privată. Serverul și clientul utilizează apoi aceeași secvență de operații pentru a manipula datele folosite pentru crearea secretului. Rezultă astfel un set de date denumit *secret master*.
7. Atât clientul cât și serverul folosesc secretul master pentru a genera cheile care vor fi utilizate în această sesiune, procesul depinzând de tipul de cifru ales pentru sesiune.

8. Începe transferul de date. Datele transferate sunt criptate folosind un algoritm simetric și cheile corespunzătoare sesiunii.

Ce pagini Web ar trebui să folosească protocolul SSL?

Datorită operațiilor suplimentare pe care le presupune criptarea, are sens să folosiți protocolul SSL numai pentru paginile Web care conțin sau solicită într-adevăr date importante sau confidențiale. Activarea SSL pentru fiecare pagină din situl dumneavoastră poate să încetinească răspunsul și să descurajeze utilizatorii să vă viziteze. Utilizând protocolul SSL numai pentru paginile Web care au cu adevărat nevoie de acest protocol, cum ar fi un formular de comandă, situl dumneavoastră Web va produce un răspuns mai rapid pentru utilizator decât în cazul în care SSL ar fi folosit pentru fiecare pagină.

FIGURA 9.2

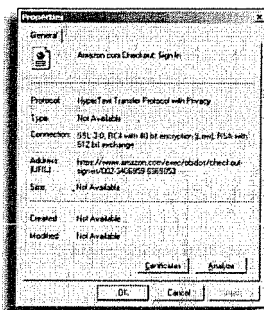
Protocolul SSL poate fi utilizat împreună cu mai multe tipuri diferite de tehnici criptografice, incluzând aici DES, RSA, MD5, RC2, RC4 și alte câteva. Această flexibilitate face ca majoritatea clienților și serverelor să fie capabili să selecteze un cifru comun și să îl folosească pentru comunicații sigure.

Această pagină Web folosește criptarea?

Înainte de a trimite numărul cărții dumneavoastră de credit sau alte informații importante în urma unei solicitări dintr-o pagină Web, este recomandat să verificați dacă pagina Web respectivă permite și folosește o formă de criptare. În Internet Explorer, căutați imaginea unui mic lacăt în partea de jos a ferestrei browserului. Pentru a afla ce tip de criptare este utilizat, executați clic cu butonul drept al mouse-ului undeva pe pagina Web și selectați opțiunea Properties. În figura 9.3 puteți vedea pagina Properties afișând câteva informații despre pagina Web, dar, mai important, și tipul de criptare folosit (în câmpul Connection).

FIGURA 9.3

Pagina Properties a unui sit Web poate fi utilizată pentru a afla tipul de criptare folosit.

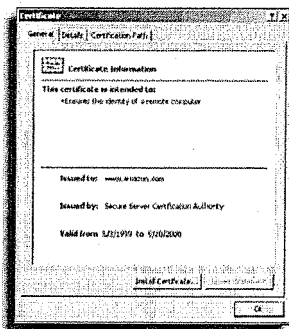
**Ce este TLS?**

TLS este prescurtarea numelui protocolului Transport Layer Security. TLS versiunea 1.0 este descris în documentul RFC 2246, „Protocolul TLS versiunea 1.0”¹. Acest protocol se bazează pe SSL 3.0 și este urmașul protocolului SSL. Diferențele dintre SSL 3.0 și TLS 1.0 sunt minore, însă suficient de semnificative pentru a împiedica interoperabilitatea acestora. Pentru mai multe informații despre noul protocol TLS, citiți documentul RFC și situl Web al comitetului IETF care lucrează la TLS, la adresa:

www.ietf.org/html.charters/tls-charter.html

FIGURA 9.4

Folosind butonul Certificates din pagina Properties, puteți vedea mai multe informații despre certificat.



Dacă doriți să aflați mai multe informații despre certificatul serverului folosit pentru această sesiune, executați clic pe butonul Certificates. În figura 9.4 este prezentată caseta de dialog Certificate, care afișează informații generale despre certificat.

Dacă executați clic pe eticheta Details din partea de sus a casetei de dialog Certificate, puteți analiza certificatul mai detaliat, aflând emitentul certificatului și algoritmi utilizați. Eticheta Certificate Path poate fi

folosită pentru a afla mai multe informații despre serverul care a emis certificatul.

Rezumat

Utilizarea criptării va rezolva trei probleme asociate cu folosirea rețelei Internet pentru transferul datelor importante. Metodele criptografice pot fi folosite pentru a autentifica părțile care comunică, pentru a verifica integritatea datelor transmise și, de asemenea, pentru a face comunicația privată, prin faptul că orice mesaj interceptat este imposibil de citit.

Tehnicile de criptare simetrice, care folosesc o singură cheie, sunt în general mai rapide decât tehnicile asimetrice, cum ar fi cele cu perechi de chei publică/secretă, care folosesc două chei între care există o relație matematică. În practică, cele două tehnici sunt utilizate deseori împreună, pentru creșterea nivelului de securitate. Exemple de tehnologii care folosesc ambele metode sunt protocolul Secure Sockets Layer (SSL) și produsul foarte popular de criptare Pretty Good Privacy (PGP), despre care vom discuta în capitolul 11.

În următorul capitol, vom analiza o aplicație practică a criptografiei: crearea rețelilor virtuale private (VPN) pentru a stabili canale sigure de comunicație în Internet. Tot în acest capitol, vom trece în revistă și alte două protocoale importante care pot fi folosite pentru a crea rețele VPN: IPSec și PPTP.

¹ În original, „The TLS Protocol Version 1.0” (n.trad.)

Capitolul 10**Rețele virtuale private (VPN) și tuneluri**

- Comunicații sigure în Internet
- Suita de protocoale IPSec
- Protocolul PPTP (Point-to-Point Tunneling Protocol)

Comunicații sigure în Internet

Dacă doriți să creați un canal sigur care să poată fi utilizat pentru comunicarea cu un birou situat la distanță, primul lucru care vă vine în minte este probabil folosirea unei linii închiriate dedicate (sau a unei linii telefonice obișnuite dacă traficul este mic și cu frecvență redusă). Însă având la dispoziție rețeaua Internet, care oferă oricum o cale rapidă între cele mai multe locații de pe glob la un preț nesemnificativ în comparație cu liniile închiriate sau taxele de trecere, nu este logic să utilizați această variantă? Ați putea spune că o conexiune pe linie telefonică sau pe linie închiriată poate să ofere mai multă securitate, deoarece datele circulă pe un traseu dedicat și nu pot fi interceptate ușor de altcineva. În Internet, nu aveți nici un control asupra direcției în care circulă pachetele pentru a fi rutate către destinație. Nu aveți nici un control asupra legăturilor dintre punctele A și B.

Există produse, cum ar fi Pretty Good Privacy (PGP), care pot fi utilizate pentru a trimite mesaje de poștă electronică și fișiere atașate prin Internet, cu o protecție care este extrem de dificil de învins. Pentru paginile Web, după cum ați văzut deja în capitolul precedent, poate fi folosit protocolul Secure Sockets Layer (SSL) pentru schimbul de informații confidențiale.

Vezi și

- Pentru mai multe informații despre utilizarea programului PGP pentru protejarea tranzacțiilor dumneavoastră de poștă electronică, vezi pagina 188.

Pentru o conexiune cu scop general, care permite ca două rețele să schimbe în mod protejat mai multe tipuri de date ce folosesc protocolul IP pentru transmisie, este necesară o altă soluție. Soluția este rețeaua virtuală privată (Virtual Private Network, sau VPN), prin care puteți crea un tunel pentru traficul de rețea dintr-o locație în alta, într-un format criptat care să ascundă datele respective de ochii curioși.

Virtual Private Network Consortium (VPNC)

Această asociație comercială a furnizorilor de produse VPN are un sit Web care poate fi util pentru cei care doresc să cunoască tehnologia VPN mai detaliat decât poate fi prezentată în acest capitol. La următoarea adresă URL, veți găsi pagina de bază a organizației VPNC:

www.vpnc.org

Acest sit Web include legături către documente despre rețelele VPN, cum ar fi pagini albe și documente oficiale de tip IETF Draft și RFC. De asemenea, vă puteți înscrie în lista lor poștală pentru a fi informat despre viitoarele dezvoltări ale tehnologiei VPN.

Ce este o rețea virtuală privată (VPN)?

O rețea virtuală privată este un tunel printr-o infrastructură de rețea partajată, de genul rețelei Internet. Este un *tunel* deoarece datele transferate sunt criptate și apoi încapsulate în pachete IP, împiedicând astfel înțelegerea pachetelor interceptate și protejând identitatea expeditorului și a destinatarului. Sunt folosite trei metode de bază pentru a crea rețele VPN cu ajutorul tehnologiei actuale:

- **Rețea la rețea** – Această variantă se realizează de obicei instalându-se un firewall sau un ruter din ultima generație la fiecare capăt folosit pentru crearea rețelei VPN.
- **Gazdă la rețea** – Un calculator situat la distanță, echipat cu software client VPN, poate să se conecteze la biroul de bază.
- **Provider ISP conectat pe linie telefonică la rețea** – Unii furnizori de servicii Internet (ISP) oferă servicii VPN pentru clienții conectați pe linie telefonică.

După cum puteți vedea, deși rețelele VPN sunt create de obicei între firewall-uri sau rutere, aceste rețele pot fi utilizate și pentru a conecta o gazdă situată la distanță la o rețea prin Internet, în condițiile în care gazda client este configurată corespunzător. În figura 10.1, puteți vedea un exemplu în care este folosită o conexiune VPN pentru a uni două rețele cu ajutorul conexiunilor Internet.

Firewall-ul din fiecare rețea ilustrată în acest exemplu este responsabil pentru criptarea și încapsularea traficului IP care este apoi rutat către cealaltă rețea. Atunci când o stație de lucru dintr-o rețea trebuie să acceseze un server din cealaltă rețea, firewall-ul preia pachetele IP ale stației de lucru client și împachetează propriul pachet IP în jurul clienților. Pachetele care sunt transmise apoi prin Internet conțin adresele sursă și destinație care identifică firewall-urile, și nu clientul sau serverul din fiecare rețea. Această caracteristică VPN vă ajută să ascundeți identitatea gazdelor din rețeaua dumneavoastră. Pachetul IP original circulă într-un format comprimat și criptat, astfel încât dacă este interceptat de o persoană neautorizată, conținutul este inutil.

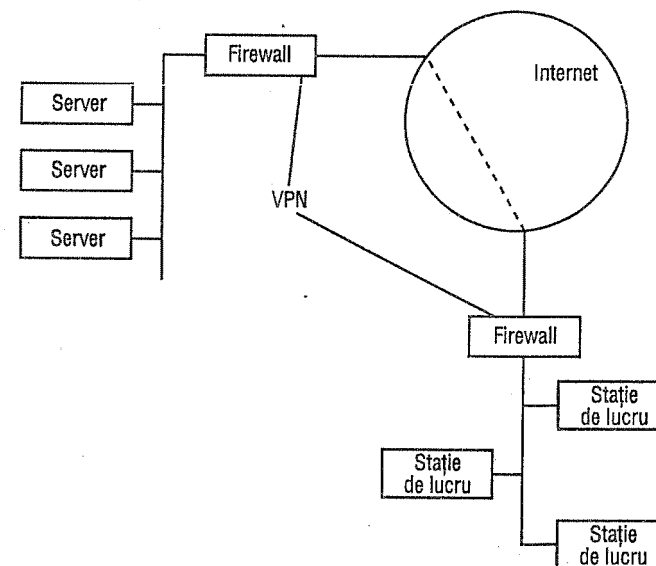
O altă caracteristică importantă oferită de rețeaua VPN este autentificarea. Cele două firewall-uri din exemplu folosesc tehnici de autentificare puternică pentru a se asigura că fiecare pachet schimbat provine cu adevărat din cealaltă parte a conexiunii.

Cele mai multe firewall-uri care suportă rețele VPN vă oferă software client care permite unui calculator gazdă individual să se conecteze pe linie telefonică la Internet și să creeze o conexiune sigură cu firewall-ul. Clienții Microsoft Windows conțin software VPN bazat pe protocolul PPTP (Point-to-Point Tunneling Protocol), despre care vom discuta într-o

secțiune următoare din acest capitol. Folosind PPTP, un client poate să se conecteze pe linie telefonică la Internet cu ajutorul unui furnizor ISP obișnuit. Clientul poate apoi să utilizeze software-ul client PPTP pentru a se conecta la un server cu acces de la distanță (RAS) din rețeaua de bază pentru stabilirea unui canal VPN sigur.

FIGURA 10.1

O rețea VPN tipică este creată între două firewall-uri.



Unii furnizori ISP oferă și o altă metodă care ar putea fi utilă pentru utilizatorii mobili. Utilizatorul de la distanță poate să apeleze furnizorul ISP pe linie telefonică și, după autentificarea corespunzătoare, furnizorul poate crea pentru utilizator o rețea VPN cu situl de la distanță. Această metodă are avantajul că utilizatorul nu trebuie să configureze nici un fel de software client pentru a crea o rețea VPN. Sunt și câteva dezavantaje: furnizorul ISP trebuie să posede linii telefonice pentru toate locațiile unde veți avea nevoie de acces, iar utilizarea unui furnizor ISP presupune că puneți o parte din gestionarea securității dumneavoastră în mâinile unei terțe părți.

Ce poate face o rețea VPN?

Rețelele VPN permit comunicații sigure pe suprafețe geografice mari. Domeniile importante în care o rețea VPN poate să aibă impact într-o organizație comercială sunt:

- Conectează filialele companiei sau siturile situate la distanță cu biroul de bază.
- Permite ca angajații să lucreze de acasă, iar utilizatorii mobili din deplasare.
- Creează o conexiune sigură cu un partener de afaceri.
- Reduce bugetul pentru telecomunicații.

Conectarea siturilor companiei situate la distanță poate costa mult atunci când folosiți linii închiriate dedicate. Puteți să utilizați conexiunea Internet existentă, împreună cu un produs firewall VPN bun, pentru a crea propriile canale private de comunicații cu filialele

situate la distanță cu mult mai puțini bani decât ar costa o linie închiriată. Dacă aveți utilizatori care lucrează în mod regulat de acasă sau angajați care călătoresc, rețelele VPN pot fi folosite pentru a securiza comunicațiile acestora cu rețeaua de la birou. Deoarece rețelele VPN pot fi implementate cu ajutorul unor conturi dial-up din Internet printr-un furnizor ISP, puteți să renunțați la cea mai mare parte din bancul de modemuri scumpe și să vă echipați utilizatorii care lucrează în afara sitului cu software client VPN. În loc să plătiți pentru mai multe linii telefonice dedicate bancului de modemuri, puteți folosi o singură conexiune Internet cu lărgime mare de bandă pentru a oferi servicii angajaților respectivi.

Vezi și

- *Windows NT și Windows 2000 includ capabilități de client VPN care pot fi utilizate împreună cu aplicația Remote Access Services pentru a crea rețele virtuale private. Pentru mai multe informații despre utilizarea software-ului client Windows VPN, vezi capitolul 21, „Firewall-uri și mai mult decât atât”, la pagina 306.*

Faxurile și serviciile de livrare nocturne lucrează fără oprire pentru a ajuta companiile să schimbe date între ele. Atunci când este absolut necesar să fie acolo – adică acum – puteți folosi în locul lor rețeaua de calculatoare. Partenerii de afaceri vor descoperi că tehnologia VPN poate să simplifice stabilirea unei conexiuni sigure între rețelele lor. Deoarece dumneavoastră folosiți un firewall pentru acest tip de rețea VPN, puteți să fiți sigur că rețeaua dumneavoastră rămâne protejată. Crearea unei rețele VPN pentru un partener de afaceri în vederea utilizării pe termen scurt poate fi de asemenea avantajoasă. Instalarea și dezinstalarea unei legături dedicate ar putea fi cu mult mai costisitoare pentru o conexiune pe termen scurt de acest tip.

Dezavantajele rețelelor VPN

Cu toate că o rețea VPN are multe avantaje față de utilizarea liniilor închiriate pentru comunicațiile la distanțe mari, există câteva lucruri care ar trebui luate în considerare atunci când se analizează avantajele și dezavantajele acestei tehnologii. În primul rând, datorită naturii rețelei Internet, în care un pachet IP poate fi rutat printr-un număr de legături intermediare mai lente sau mai rapide, viteza rețelei VPN este limitată la cea mai lentă legătură prin care este rutat traficul propriu.

În al doilea rând, când folosiți rețeaua Internet, nu controlați echipamentele hardware care preiau pachetele dumneavoastră de rețea și le mută dintr-un loc în altul. O defecțiune hardware majoră în orice punct al legăturii poate duce la întârzieri sau chiar la blocări ale rețelei. Dacă folosiți o soluție cu linie închiriată, contractul dumneavoastră poate să specifice niveluri ridicate de servicii și un timp scurt de răspuns în cazul apariției unor probleme. Utilizând rețeaua Internet, nu puteți primi acest tip de garanție.

Dacă utilizatorii dumneavoastră mobili sau situați la distanță folosesc furnizori ISP locali pentru acces pe linia telefonică în vederea utilizării software-ului client VPN pentru conexiunea cu biroul de bază, ar trebui să vă asigurați de calitatea serviciilor oferite de furnizorul ISP. Dacă liniile ISP sunt ocupate, utilizatorul trebuie să recurgă la vechea metodă de acces prin modem. Cu toate că rețelele VPN pot fi o metodă eficientă și necostisitoare de permitere a conectării câtorva utilizatori de la distanță la rețeaua dumneavoastră în comparație cu prețul întreținerii unui banc de modemuri, s-ar putea să

nu fie soluția cea mai bună. Dacă aveți un număr foarte mare de utilizatori la distanță, s-ar putea să fie mai ieftin să folosiți un banc de modemuri decât să plătiți taxele necesare pentru stabilirea unui cont dial-up ISP pentru fiecare utilizator.

În restul capitolului vor fi prezentate două protocoale importante utilizate pentru crearea de rețele VPN bazate pe standarde.

Suita de protocoale IPSec

Pe parcursul acestei cărți, am discutat de mai multe ori despre faptul că suita de protocoale TCP/IP nu a fost proiectată cu funcții de securitate. Următoarea generație a protocolului IP, denumită IPv6, va avea încorporate mecanisme de securitate. Versiunea curentă, IPv4, pe care o folosiți în Internet, nu posedă astfel de mecanisme. Datorită acestui fapt, a fost dezvoltat un standard nou, denumit IPSec, pentru satisfacerea acestor cerințe de securitate. IPSec va exista obligatoriu în IPv6, dar poate fi implementat în mod transparent și în rețeaua Internet curentă, care este bazată pe IPv4.

Vezi și

- *Pentru mai multe informații despre protocolul IP din următoarea generație – IPv6 – vezi capitolul 21, „Firewall-uri și mai mult decât atât”, la pagina 306.*

Documente RFC despre IPSec

Pentru a afla mai multe detalii despre IPSec, puteți citi documentele RFC din Internet. RFC 1825, „Arhitectura de securitate pentru protocolul Internet”¹, vă oferă o prezentare generală. Iată și alte documente:

RFC 1826, „Antetul de autentificare”²

RFC 1827, „IP Encapsulating Security Payload (ESP)”

RFC 1828, „Autentificarea IP folosind algoritmul MD5 cu cheie”³

RFC 1829, „Transformarea ESP DES-CBC”⁴

Aceste documente vă vor oferi mai multe informații referitoare la modul în care funcționează diferitele componente care formează IPSec.

IPSec este adoptat de un număr din ce în ce mai mare de furnizori de firewall-uri pentru înlocuirea metodelor particulare folosite în trecut pentru criptare. Există câteva motive întemeiate care vă pot conduce la concluzia că, în viitorul apropiat, IPSec va fi implementat puternic în Internet:

- IPSec este un standard. Pe lângă documentele RFC care definesc arhitectura și componentele importante ale suitei IPSec, există multe alte documente Internet și RFC scrise pentru a standardiza metodele criptografice care pot fi utilizate și alte protocoale care au legătură cu IPSec.

¹ În original, „Security Architecture for the Internet Protocol” (n.trad.)

² În original, „The Authentication Header” (n.trad.)

³ În original, „IP Authentication using Keyed MD5” (n.trad.)

⁴ În original, „The ESP DES-CBC Transform” (n.trad.)

- IPSec este transparent pentru utilizator și pentru generația curentă de echipamente de rutare care asigură legăturile în Internet. IPSec operează la nivelul rețea, deci nu trebuie modificate aplicațiile sau structura fizică de bază a rețelei de calculatoare.

- IPSec este flexibil. Poate fi utilizat împreună cu o mare varietate de metode criptografice.

IPSec nu este un singur protocol. La fel ca TCP/IP, este o suită de protocoale între care există legături. Cele trei componente principale care formează baza suitei IPSec sunt următoarele:

- **Internet Key Exchange (IKE)** – Acest protocol este utilizat în etapa de negociere inițială pentru a se pune de acord metodele de criptare, cheile și alte date care vor fi folosite pentru a configura o sesiune sigură.
- **Authentication Header (AH)** – Este un antet de securitate inserat în fiecare pachet IP și care poate fi folosit pentru a determina dacă pachetul a fost modificat în cursul tranzitului și pentru a autentifica expeditorul datelor. AH nu criptează zona de date utile a pachetului IP, ci garantează validitatea conținutului acestuia.
- **Encapsulation Security Payload (ESP)** – Pentru a asigura comunicații private, ESP criptează zona de date utile a pachetului IP, împreună cu alte informații de antet.

Internet Key Exchange (IKE)

După cum se spune în protocoalele SSL, înainte de a putea începe comunicații sigure, criptate, este nevoie de o metodă de negociere a metodelor de criptare utilizate și de o metodă pentru schimbul de al chei. În cazul suitei IPSec, protocolul Internet Key Exchange (IKE) este folosit pentru schimbul de date în timpul fazei inițiale de configurare a unei conexiuni securizate. IKE este utilizat pentru a decide ce metode de criptare și ce chei vor fi folosite. De asemenea, IKE ține evidența tuturor conexiunilor securizate, folosind un concept denumit *asociere de securitate* (*security association*). În documentul RFC 2408, „Asocierea de securitate în Internet și protocolul de gestionare a cheilor”¹, o asociere de securitate este definită în linii mari ca „o relație între două sau mai multe entități care descrie modul în care entitățile vor utiliza serviciile de securitate pentru a comunica în mod sigur”.

IKE este o combinație între ISAKMP și părți din metoda de schimb al cheilor Oakley. ISAKMP definește formatul pachetelor utilizate pentru a crea și gestiona asocieri de securitate. Una dintre cele mai importante caracteristici ale protocolului IKE este independența de metoda particulară de criptare pe care doriți să o folosiți pentru autentificare sau criptarea datelor. IKE definește o procedură pentru schimbul de informații, într-un mod securizat, care poate fi folosită cu mai multe metode criptografice diferite. Pentru IPSec, IKE este componenta care stabilește o asociere de securitate și gestionează toate asocierile de securitate de pe o anumită gazdă.

Metoda de schimb al cheilor Oakley

Pentru a afla mai multe despre metoda de schimb al cheilor Oakley, care este folosită de suitele IPSec, citiți documentul RFC 2412, „Protocolul de determinare a cheilor Oakley”².

¹ În original, „Internet Security Association and Key Management Protocol (ISAKMP)” (n.trad.)

² În original, „The Oakley Key Determination Protocol” (n.trad.)

Fiecare asociere de securitate este unidirecțională. Pentru ca două gazde să comunice în siguranță, sunt necesare două asocieri de securitate, câte una pentru fiecare direcție. Asocierea de securitate descrie atribute importante pentru fiecare conexiune, cum ar fi:

- **Algoritmii criptografici** – Fiecare asociere negociază metodele specifice de criptare care vor fi folosite pentru sesiunea curentă.
- **Cheile** – Acestea sunt cheile negociate sau generate de părțile care formează asocierea.
- **Frecvența cu care vor fi schimbate cheile noi** – Utilizarea cheilor de sesiune numai pentru o perioadă limitată de timp îmbunătățește securitatea sistemului.
- **Durata de validitate a asocierii de securitate** – Asocierea de securitate nu ar trebui să mai existe după ce dispăre nevoia pentru o sesiune securizată.
- **Adresa sursă a asocierii de securitate** – Deoarece asocierile de securitate sunt unidirecționale, adresa sursă a părții care a inițiat asocierea de securitate este folosită pentru a identifica asocierea respectivă.
- **Indexul parametrului de securitate (Security Parameter Index, sau SPI)** – Acesta este un număr de 32 de biți, folosit pentru a identifica în mod unic asocierea de securitate.
- **Alte informații** – Aici sunt incluse orice date importante pentru asociere și metodele criptografice alese pentru utilizare.

Protocolul IKE are mai multe moduri de operare pentru a configura o asociere. În *modul principal* (*main mode*), IKE creează un canal securizat cu o gazdă situată la distanță, ce va fi folosit pentru negocierile următoare. Pentru a crea conexiunea sigură, nodul care inițiază conexiunea trimite o listă de parametri pe care îi propune pentru asociere, incluzând algoritmi de criptare și hashing, o metodă de autentificare, dacă securitatea dorită va folosi tehnicile Authentication Header sau Encapsulation Security Payload și alte date necesare. Folosind metode cu chei publice, cele două părți ale sesiunii sunt autentificate una în fața celeilalte. Pentru autentificare sunt utilizate certificate digitale.

Destinatarul certificatului poate verifica în primul rând dacă certificatul corespunde cu gazda de la celălalt capăt al conexiunii și apoi dacă acel certificat este valabil, fiind emis de o autoritate de certificare recunoscută (CA).

A doua metodă de începere a configurării unei asocieri de securitate este denumită *mod agresiv* (*aggressive mode*). Principala diferență dintre modulele principal și agresiv este aceea că a doua metodă operează cu mai puține schimburi de date între părți, având mai multe informații transferate în timpul fiecărui schimb. Datorită acestui fapt, modul agresiv nu este la fel de atent ca modul principal și nu protejează identitatea părților în rețea. Indiferent de modul folosit, ambele au ca rezultat o asociere de securitate care va fi folosită de protocolul IKE (prescurtat, *IKE SA*). După realizarea asocierii, protocolul IKE poate fi utilizat pentru a configura asocierea de securitate curentă de care au nevoie gazdele pentru un canal sigur de comunicații.

După faza inițială a modului principal sau agresiv, este introdus un alt mod, denumit *mod rapid* (*quick mode*), pentru negocierea serviciilor care vor fi folosite și pentru generarea cheilor de sesiune. Deoarece între părți a fost stabilit deja un canal sigur de comunicații în timpul configurării inițiale, pachetele utilizate pentru modul rapid pot circula criptate prin rețea. Un mesaj de mod rapid este trimis pentru a solicita configurarea unei asocieri de securitate. Ca răspuns, sunt configurate două asocieri de securitate, câte una pentru fiecare

direcție dintre gazdele care negociază canalul. Partea de la capătul destinat al fiecărei asocieri de securitate unidirecțională răspunde de alegerea unui număr unic ce va fi folosit pentru indexul SPI al asocierii și îl comunică inițiatorului asocierii.

Când protocolul IKE este utilizat pentru a crea asocierile de securitate necesare, există două tehnici puse la dispoziție de suita IPSec și care pot fi folosite pentru a proteja sau a transmite comunicațiile private între cele două gazde.

Învățați mai multe lucruri despre IKE și ISAKMP

Ar fi necesare câteva capitole pentru a prezenta toate detaliile referitoare la IKE și ISAKMP. Dacă doriți să aflați mai mult, vă recomand să citiți următoarele documente RFC care descriu componentele individuale:

RFC 2408, „Asocierea de securitate în Internet și protocolul de gestionare a cheilor”

RFC 2409, „Protocolul Internet Key Exchange (IKE)”¹

RFC 2412, „Protocolul de determinare a cheilor Oakley”

Authentication Header (AH)

Această metodă nu asigură criptarea zonei propriu-zise de date utile a pachetului IP, astfel încât utilizarea antetului de autentificare (Authentication Header, sau AH) de sine stătător nu va oferi confidențialitate. AH vă oferă o metodă prin care să determinați dacă datele conținute de pachet sau informațiile importante din antet au fost modificate pe parcursul tranzitului, precum și autentificarea expeditorului.

Pentru protocolul IPv4, AH inserează în pachet propriul antet, chiar după antetul IP (vezi figura 10.2). Deoarece antetul IP este nemodificat, ruterele care nu sunt familiarizate cu suita de protocoale IPSec pot continua să ruteze pachetele așa cum procedează în mod obișnuit.

FIGURA 10.2

Antetul de autentificare este plasat chiar după antetul de pachet IP pentru protocolul IPv4.

Antetul IP versiunea 4	Antetul AH	Protocol de nivel superior, cum ar fi TCP sau UDP
------------------------	------------	---

FIGURA 10.3

Câmpurile din antetul de autentificare.

8 biți	8 biți	16 biți
Antetul următor	Lungime	Zonă rezervată
Indexul parametrilor de securitate (SPI)		
Numărul de secvență		
Date de autentificare (un număr variabil de cuvinte pe 32 de biți)		
32 de biți		

Antetul AH este format din cinci câmpuri de lungime fixă, urmate de datele de autentificare, care variază în lungime datorită cantității variabile de informații care trebuie incluse pentru metodele de autentificare și criptografice alese (vezi figura 10.3).

Câmpurile de informații din antetul AH sunt următoarele:

- **Antetul următor (Next Header)** – Acest câmp de 8 biți identifică protocolul care urmează după antetul AH. Este un număr valid de protocol IP, așa cum este definit de organizația IANA. De exemplu, dacă un pachet TCP urmează după antetul AH, aici este identificat TCP. Dacă ESP este folosit în combinație cu antetul AH, ESP este protocolul identificat aici.
- **Lungime (Length)** – Acest câmp de 8 biți specifică lungimea antetului AH ca număr de cuvinte de 32 de biți.
- **Zonă rezervată (Reserved)** – Acest câmp nu este folosit în mod curent, însă, în funcție de standard, ar trebui să fie completat cu zerouri.
- **Indexul parametrilor de securitate (Security Parameters Index, sau SPI)** – Acest număr de 32 de biți este ales de capătul destinat al unei asocieri de securitate pentru a identifica în mod unic asocierea de securitate. Valoarea zero indică faptul că nu există nici o asociere de securitate. Numerele de la 1 la 255 sunt rezervate de organizația IANA.
- **Numărul de secvență (Sequence number)** – Acesta este un contor care crește cu fiecare pachet trimis pentru un anumit număr SPI.
- **Date de autentificare (Authentication Data)** – Acest câmp conține datele propriu-zise ale pachetului, cum ar fi, de exemplu, semnătura digitală. Câmpul este completat până la o lungime egală cu un număr fix de cuvinte de 32 de biți.

Chiar dacă antetul AH poate fi folosit pentru autentificare și pentru a garanta integritatea datelor transmise între cele două părți care cooperează, nu poate fi utilizat pentru a cripta datele propriu-zise din pachetul IP. Pentru aceasta este folosită o altă tehnică.

Ce câmpuri din antetul IP protejează metoda AH?

Metoda Authentication Header folosește calcule criptografice efectuate asupra datelor din datagrama IP, excluzând câmpurile care se modifică pe durata transportului, cum este câmpul pentru durata de viață (TTL). Datagrama poate fi evaluată la capătul destinat pentru a determina dacă a fost modificată. Informațiile care nu suferă modificări, cum sunt adresele sursă și destinație, sunt protejate de metoda AH.

Encapsulation Security Payload (ESP)

Metoda Encapsulation Security Payload (ESP) asigură, pe lângă autentificarea și integritatea datagramelor, și criptarea datelor conținute de datagramă. În *modul transport*, ESP asigură protecția datelor și anteturilor create de protocoalele de nivel superior (cum este TCP). ESP nu oferă protecție pentru antetul IP propriu-zis. Acest mod este folosit de obicei pentru implementările gazdă-la-gazdă (sau conexiunile gazdă-la-poartă) și este compatibil cu ruterele care nu înțeleg protocoalele IPSec.

În *modul tunel*, ESP este utilizat între două porți, cum ar fi două firewall-uri, și protejează informațiile din antetul IP. În acest mod, întreaga datagramă IP este încapsulată de protocolul ESP, iar noile informații de antet aplicate specifică porțile de securitate între care este trimis pachetul. Adresele efective de la punctele finale ale comunicației sunt conținute în informațiile criptate din antet, transportate acum ca parte a zonei de date utile a pachetului. Când pachetul ajunge la poarta destinație, este despachetat și trimis către gazda destinație reală.

¹ În original, „The Internet Key Exchange (IKE)” (n.trad.)

Metodele AH și ESP

Metodele AH și ESP pot fi folosite împreună pentru a obține un canal de comunicații sigur și solid. În această variantă sunt asigurate autentificarea, integritatea și confidențialitatea. Când sunt folosite împreună, antetul AH urmează antetului IP, iar în continuarea antetului AH este pachetul IP încapsulat după metoda ESP.

Protocolul PPTP (Point-to-Point Tunneling Protocol)

Majoritatea persoanelor care au acasă o conexiune Internet au o idee referitoare la ce este PPP: Point-to-Point Protocol. PPP este un protocol care încapsulează alte protocoale (cum ar fi TCP/IP, IPX sau NetBEUI) și le retransmite între furnizorul ISP și calculatorul dumneavoastră de acasă. Protocolul PPTP (Point-to-Point Tunneling Protocol) este construit pe baza protocolului PPP prin adăugarea funcției de criptare a datelor încapsulate. Aceasta înseamnă că PPTP poate fi utilizat de clienții situați la distanță sau mobili care au nevoie să creeze o conexiune virtuală privată prin rețeaua Internet (care nu este sigură) până la rețeaua de la biroul de bază.

Între avantajele utilizării protocolului PPTP se numără:

- Un canal criptat de comunicații prin Internet.
- Suport pentru încapsularea mai multor protocoale de rețea, cum ar fi TCP/IP, SPX și NetBEUI.
- Software-ul pentru PPTP este încorporat în cele mai recente sisteme de operare Windows.
- Permite folosirea adreselor IP private, deoarece conexiunea PPP utilizează adresa IP atribuită de furnizorul ISP; clientul poate să trimită pachetele prin tunel folosind o adresă de rețea validă în rețeaua de bază.

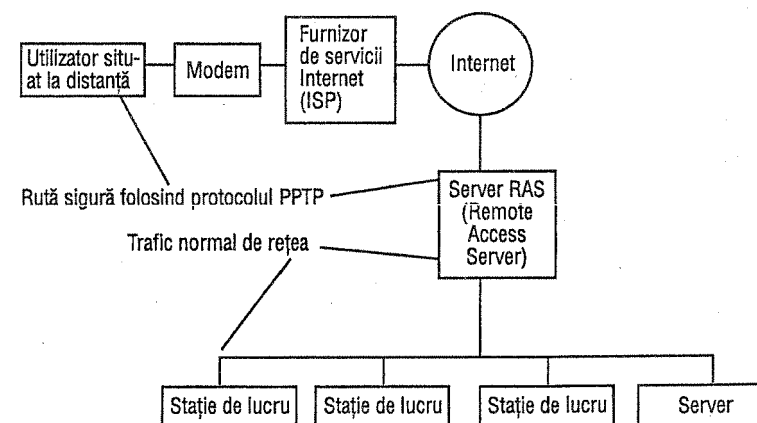
PPTP a fost dezvoltat inițial de firma Microsoft și de alte câteva companii. Forumul PPTP a prezentat un document Internet Draft comitetului IETF (Internet Engineering Task Force) în 1996, iar documentul RFC 2637, „Protocolul PPTP (Point-to-Point Tunneling Protocol)”¹, definește standardul curent pentru protocol.

Într-un scenariu tipic, un client situat la distanță realizează inițial o conexiune cu un furnizor ISP local folosind protocolul PPP (vezi figura 10.4). După stabilirea acestei conexiuni, este creată a doua conexiune pentru PPTP peste această conexiune PPP. Punctele finale ale conexiunii PPTP sunt utilizatorul situat la distanță și un server RAS (Remote Access Server) din rețeaua destinație a utilizatorului. Conexiunea dintre utilizatorul situat la distanță și serverul RAS este numită *tunel*, iar toate datele care sunt transferate între cele două puncte finale sunt criptate și protejate de PPTP. La nivelul serverului RAS, pachetele PPTP sunt despachetate, iar datagrama IP originală (sau datagramele altor protocoale de rețea) sunt evaluate și trimise către destinațiile lor reale din rețeaua locală deservită de serverul RAS.

¹ În original „Point-to-Point Tunneling Protocol (PPTP)” (n.trad.)

FIGURA 10.4

Un client situat la distanță folosește un tunel PPTP între stația de lucru și serverul RAS din rețeaua de bază.



Pentru a stabili o conexiune PPTP sigură, este stabilită o conexiune de control, iar transmisia de date poate începe.

Conexiunea de control PPTP

Mesajele de control sunt trimise între clientul PPTP și serverul PPTP pentru a crea și a gestiona tunelul PPTP. Deși protocolul PPTP poate fi folosit împreună cu PPP pentru a trimite prin tunel mai multe protocoale de rețea, PPTP utilizează o datagramă TCP pentru mesajele de control. Între clientul și serverul PPTP este stabilită o conexiune TCP prin care sunt schimbate mesaje de control PPTP. Mesajele care pot fi utilizate pe această conexiune de control sunt următoarele:

- Start-Control-Connection-Request (Cerere de începere a conexiunii de control)
- Start-Control-Connection-Reply (Răspuns de începere a conexiunii de control)
- Stop-Control-Connection-Request (Cerere de terminare a conexiunii de control)
- Stop-Control-Connection-Reply (Răspuns de terminare a conexiunii de control)
- Echo-Request (Cerere de ecou)
- Echo-Reply (Răspuns de ecou)
- Outgoing-Call-Request (Cerere de apel către exterior)
- Outgoing-Call-Reply (Răspuns la un apel către exterior)
- Incoming-Call-Request (Cerere de apel către interior)
- Incoming-Call-Reply (Răspuns la un apel către interior)
- Incoming-Call-Connected (Apel către interior conectat)
- Call-Clear-Request (Cerere de anulare a unui apel)
- Call-Disconnect-Notify (Notificare privind deconectarea unui apel)
- WAN-Error-Notify (Notificare privind o eroare WAN)
- Set-Link-Info (Informații privind stabilirea legăturii)

Mesajul de cerere a începerii sesiunii și mesajul de răspuns asociat sunt folosite pentru a începe o conexiune și pentru a schimba date despre capabilitățile clientului și serverului. Între acestea se numără informații cum ar fi versiunea PPTP, numărul maxim de sesiuni individuale care pot fi suportate și numele de gazdă DNS al solicitantului. Mesajele de terminare a conexiunii sunt folosite pentru a încheia o conexiune PPTP. Când este terminată o conexiune de control, sunt terminate toate sesiunile asociate cu tunelul pus la dispoziție de conexiunea de control.

Mesajele de ecou sunt folosite pentru întreținerea conexiunii de control, astfel încât o defecțiune la unul dintre capete să poată fi detectată după o perioadă de timp, iar conexiunea să poată fi întreruptă. O conexiune este terminată dacă nu este recepționat nici un răspuns la o cerere de ecou în termen de 60 de secunde.

După stabilirea unei conexiuni de control între client și server, sunt folosite diferite tipuri de mesaje de apel pentru stabilirea de sesiuni între cele două puncte finale.

Și mesajul de notificare privind o eroare WAN poate fi folosit pentru a schimba informații despre conexiune.

Transmisii de date care utilizează tunelul PPTP

După stabilirea unei conexiuni, există un tunel virtual care poate fi utilizat pentru a schimba date între clientul și serverul PPTP. Pachetul PPTP trimis de client este inițial criptat și apoi încapsulat într-un pachet IP care poate fi rutat către serverul PPTP. Deoarece pachetul IP original este criptat, poate fi trimis în siguranță prin Internet. Dacă pachetul IP care încapsulează pachetul PPP este interceptat, nu pot fi înțelese decât informațiile din antetul IP. Datele conținute în pachetul PPP sunt protejate de criptarea folosită.

O diferență între metoda de lucru cu tunel folosită de PPTP și cea folosită de IPSec este următoarea: în timp ce IPSec utilizează o asociere de securitate diferită pentru fiecare sesiune dintre un client și server, PPTP utilizează un singur tunel și mai multe sesiuni între client și server în același tunel.

Protocolul L2TP (Layer Two Tunneling Protocol)

Un standard nou pentru tehnologia VPN este realizat prin combinarea celor mai bune părți ale protocoalelor PPTP și L2F produs de Cisco: Layer Two Tunneling Protocol (L2TP). Acest protocol a fost descris recent într-un document cu evidența protocoalelor standard din Internet, RFC 2661, „Protocolul Layer Two Tunneling Protocol (L2TP)”¹. Pe măsură ce această tehnologie va fi dezvoltată, vă puteți aștepta să vedeți folosirea sa în software-ul VPN pentru client și server. Dacă vă interesează viitoarele dezvoltări ale acestui protocol, vizitați pagina de bază a grupului de lucru IETF care a stabilit următoarele extensii ale protocolului:

<http://www.ietf.org/html.charters/l2tpext-charter.html>

¹ În original, „Layer Two Tunneling Protocol (L2TP)” (n.trad.)

Rezumat

Rețelele virtuale private permit organizațiilor să creeze canale de comunicații securizate și private prin rețele nesigure, de genul Internet. Folosirea conexiunilor VPN poate fi mai puțin costisitoare pentru legarea birourilor situate la distanțe geografice mari și pentru cei care au mare nevoie să conecteze utilizatori de la distanță sau mobili. În prezent, pentru crearea de rețele VPN care se bazează pe standarde sunt folosite pe scară largă protocoalele IPSec și PPTP în locul soluțiilor particulare care erau utilizate în trecut. Prin dezvoltarea de standarde, vor putea fi create rețele VPN cu ajutorul unor produse software și hardware de la furnizori diferiți. În viitorul apropiat, rețelele VPN vor fi o caracteristică obișnuită a Internetului.

Utilizarea programului PGP (Pretty Good Privacy) pentru criptare

- Transferuri de informații de securitate în Internet
- Instalarea programului PGP

Securizarea transferurilor de informații în Internet

În precedentele două capitole, am discutat despre criptare și rețele virtuale private (VPN). Înainte ca Internetul să poată deveni un mediu prin care persoanele obișnuite să aibă încredere să transmită informații confidențiale – cum ar fi numărul unei cărți de credit – va fi necesar ca oamenii să fie convinși că astfel de informații pot fi criptate într-un mod care le face incredibil de greu de interceptat. Deși puteți să folosiți rețelele VPN și alte tehnici pentru a vă conecta rețeaua la un sit de la distanță, s-ar putea să nu fie o soluție practică în cazul în care aveți de-a face cu clienți sau furnizori. Pentru astfel de situații, ar trebui să luați în considerare utilizarea unui instrument de criptare foarte apreciat, cum este utilitarul Pretty Good Privacy (PGP).

PGP, care a fost dezvoltat inițial de Phillip Zimmerman, este un sistem de criptare cu chei publice. Cea mai răspândită versiune se bazează pe tehnologia brevetată denumită criptare cu chei publice RSA. Denumirea RSA vine de la inițialele dezvoltatorilor acestei tehnologii: Rivest, Shamir și Adelman. Deoarece PGP se bazează pe o tehnologie brevetată, trebuie să îl cumpărați dacă doriți să îl folosiți în scop comercial. Puteți totuși obține o copie gratuită pentru utilizarea personală nonprofit, de la Networks Associates, la următoarea adresă URL:

http://www.nai.com/default_pgp.asp

În acest sit de descărcare, veți găsi PGP atât sub formă de cod sursă (pentru sistemele UNIX), cât și ca programe executabile pentru câteva platforme de sisteme de operare diferite, cum ar fi Windows, DOS și Macintosh. În funcție de preferințele dumneavoastră, puteți folosi interfața în linie de comandă a programului PGP sau interfața grafică (GUI) oferită de acest program.

Versiunile gratuite (freeware) disponibile la Network Associates sunt oferite pentru următoarele platforme:

- Windows NT, Windows 95 /98 (în formă executabilă, interfață grafică sau în linie de comandă)
- Macintosh (executabil și cod sursă, interfață grafică)

- Linux (executabil, linie de comandă)
- Solaris (executabil, linie de comandă)
- DOS sau UNIX (cod sursă, linie de comandă)

Patentul RSA

La data publicării acestei cărți, patentul RSA era încă valabil. Însă spre sfârșitul anului 2000, patentul trebuia să expire, iar tehnicile de criptare protejate de patent să devină publice.

Instalarea programului PGP

Metoda pe care o folosiți pentru a instala programul PGP depinde de sistemul de operare utilizat. În acest capitol, vor fi prezentate tehnicile de instalare pentru UNIX și Windows NT.

Instalarea programului PGP pe sistemele UNIX

Pentru a instala programul PGP pe un sistem UNIX, inițial trebuie să compilați codul sursă și apoi să îl plasați în directorul corespunzător. Puteți apoi configura PGP pentru utilizare prin crearea perechii de chei publică și personală.

După ce despachetați fișierul `.tar1`, citiți fișierul text `setup.doc`. Acest fișier conține instrucțiunile pentru compilarea programului PGP pe diferite variante de UNIX sau Linux. După ce compilați codul sursă, va trebui să creați un director care să fie folosit exclusiv pentru PGP și să definiți o variabilă de mediu `PGPPATH` care să indice acest director. De exemplu:

```
#mkdir .pgp
#setenv PGPPATH /user/ogletree/.pgp
```

De asemenea, puteți să adăugați această definiție în fișierul `~/.csh_env` pentru a nu fi nevoit să o introduceți ulterior din nou. În continuare, trebuie să generați perechea de chei publică/personală pe care o veți folosi. Pentru aceasta este utilizată opțiunea `-k` a comenzii PGP:

```
# pgp -kg
```

Definirea unei variabile de mediu

Diferitele versiuni de UNIX folosesc metode diferite pentru definirea variabilelor de mediu și fișiere de pornire diferite pentru memorarea acestora. De exemplu, atunci când utilizați nucleul bash, trebuie să adăugați următoarele linii în fișierul `~/.sh_env`:

```
PGPPATH=/user/ogletree/.pgp;
export PGPPATH
```

Pentru a obține datele de care are nevoie pentru a efectua această funcție, PGP vă va cere câteva informații suplimentare:

¹ tar = program de comprimare în sistemele de operare UNIX (n.trad.)

- **Mărimea cheii** – Cu cât este mai mare dimensiunea cheii specificate, cu atât vor fi mai sigure datele dumneavoastră. Puteți să introduceți 1 (512 biți), 2 (768 de biți) sau 3 (1024 de biți) sau orice alt număr în afara cifrelor de la 1 la 3, pentru a preciza o anumită lungime a cheii.
- **Identificatorul utilizatorului cheii** – Acesta este numele care va fi folosit pentru a face referire la cheie. O metodă răspândită de denumire a cheii este folosirea numelui dumneavoastră urmat de adresa dumneavoastră de poștă electronică închisă între paranteze unghiulare. De exemplu, Terry W. Ogletree <ogletree@bellsouth.net>.
- **Fraza de trecere** – Fraza de trecere este folosită de PGP pentru a ajuta la generarea perechii de chei. Termenul *frază* este folosit deoarece nu este un singur cuvânt, ca în cazul parolei, ci o expresie mai lungă, pentru a face cheia mai sigură. Textul pe care îl introduceți pentru fraza de trecere nu va fi afișat pe ecran, astfel încât PGP vă va invita să-l reintroduceți, pentru a confirma că ați scris la tastatură exact ceea ce ați intenționat. Nu uitați că în toate utilitățile UNIX se face deosebire între literele mari și mici. Rețineți nu numai fraza de trecere, ci și modul în care ați introdus-o.
- **Tastare aleatoare** – PGP vă va cere să începeți scrierea de la tastatură în mod aleator. Puteți scrie ce caractere doriți; textul pe care l-ați introdus nu contează. PGP folosește în schimb intervalele de timp dintre apăsările de taste pentru a genera o serie de numere aleatoare care vor fi folosite pentru a ajuta la crearea perechii de chei. Când auziți un sunet „bip“, PGP a terminat măsurarea intervalului de timp dintre apăsările de taste și vă puteți opri.

Vezi și

➤ Pentru mai multe informații despre chei, citiți capitolul 9, „Tehnologii de criptare“, la pagina 166.

După ce primește răspunsuri la aceste cereri, programul PGP generează perechea de chei publică/personală. Această operație poate dura mai mult și depinde de dimensiunea cheii solicitate.

Nu uitați fraza de trecere!

Fraza de trecere o folosiți pentru a avea acces la cheia dumneavoastră secretă, la fel cum o parolă este folosită pentru a obține acces la contul de utilizator din rețea. Ca urmare, când luați decizia privind fraza pe care o veți folosi, ar trebui să fie ceva de care să vă amintiți ușor, dar nu chiar așa de obișnuită încât alte persoane să o ghicească ușor.

Inelele cu chei

Pentru a păstra cheile, programul PGP folosește un fișier denumit *inel cu chei* (*key ring*). Acest fișier, denumit *key.asc*, păstrează nu numai cheile dumneavoastră publică/personală, ci și cheile pe care le primiți de la alte persoane cu care doriți să comunicați. Pentru a garanta securitatea acestui fișier, ar trebui să vă gândiți la salvarea sa pe o dischetă și păstrarea acesteia încuiată până când veți avea nevoie de fișier. Dacă stocați fișierul pe hard discul local sau pe o unitate de rețea, este mai susceptibil pentru a fi compromis.

Pe lângă utilizarea fișierului inel cu chei, puteți folosi pentru a obține sau a păstra chei unul dintre numeroasele servere cu chei publice existente în Internet. Aceasta simplifică obținerea cheii dumneavoastră publice de către alte persoane atunci când dorec să vă

trimită un mesaj e-mail, de exemplu. În Internet există o rețea de servere cu chei pe care puteți să vă „publicați“ cheia proprie. Acest lucru se face prin extragerea cheii într-un fișier și trimiterea ei la unul dintre serverele cu chei. Serverele, care fac parte din rețeaua de servere cu chei, se actualizează în mod regulat unul pe celălalt, astfel că nu trebuie să trimiteți cheia la toate serverele, ci doar la unul dintre ele.

Pentru mai multe informații privitoare la serverele PGP cu chei publice și comenzi folosite pentru a avea acces la ele, trimiteți un mesaj care să conțină textul *help* în linia de subiect, la adresa *pgp-public-keys@keys.pgp.net*.

Comenzi PGP

La început, haideți să analizăm comanda pe care o folosiți pentru a extrage cheia dumneavoastră publică astfel încât să o puteți oferi celorlalți:

```
#pgp -kx userid keyfile [key ring]
```

În acest exemplu, *userid* este numele pe care l-ați dat cheii, iar *keyfile* este numele fișierului în care doriți să plaseze cheia programul PGP. Acest fișier de ieșire conține o copie a cheii dumneavoastră publice și este fișierul pe care îl oferiți celor care doresc să vă trimită mesaje. Argumentul *key ring* din comandă este opțional și este folosit dacă aveți mai multe fișiere inel cu chei.

Pentru a adăuga o cheie publică în fișierul inel cu chei, folosiți următoarea comandă:

```
#pgp -ka filename
```

În această comandă, *filename* este numele fișierului care conține cheia publică a persoanei respective.

Pentru a vizualiza conținutul inelului dumneavoastră cu chei, utilizați comanda:

```
#pgp -kvv
```

Această comandă afișează informațiile privind cheile pe care le aveți în fișierul inel cu chei.

Pentru a șterge din fișier o cheie, folosiți următoarea comandă:

```
#pgp -kr
```

Până în acest moment, ați analizat comenzile de „întreținere“ sau de „gestiune internă“ oferite de programul PGP. Însă adevărata funcție a acestui program este criptarea de fișiere, astfel că în continuare vom vedea cum este realizată această funcție.

La început, creați mesajul pe care doriți să îl criptați și salvați-l într-un fișier. Puteți folosi orice editor de texte UNIX sau un program de prelucrare de texte. Desigur, puteți să criptați și fișiere binare, cum ar fi programe executabile sau fișiere grafice. După ce obțineți fișierul pe care doriți să îl criptați, utilizați următoarea comandă:

```
#pgp -e messagefile userid
```

Argumentul *-e* comunică programului PGP să creeze fișierul specificat de dumneavoastră (*messagefile*) utilizând cheia publică pentru persoana reprezentată de *userid*. Fișierul rezultat în urma comenzii de criptare este un fișier binar. Deoarece unele programe de poștă electronică sau alte programe nu agreează folosirea fișierelor binare, s-ar putea să fie nevoie să folosiți o altă comandă pentru a crea un fișier folosind un format denumit *Blindaj ASCII* (*ASCII Armor*), care este același fișier binar codat cu caractere ASCII. Acest rezultat se obține prin atașarea opțiunii *-e* la argumentul *-e*:

```
#pgp -ea messagefile userid
```

Fișierul rezultat este format doar din text ASCII standard, cu care pot lucra majoritatea programelor de poștă electronică.

Utilizarea programului PGP pentru a crea o semnătură digitală

Operația de criptare a unui fișier nu rezolvă decât o parte a problemei protejării comunicațiilor. Deși criptarea vă protejează textul de altcineva cu excepția destinatarului, nu oferă nici o garanție destinatarului cu privire la originea textului respectiv. Astfel, dacă primiți un fișier, cum puteți fi sigur că acesta vine cu adevărat de la persoana de la care pretinde că vine? Este foarte simplu de falsificat o adresă de poștă electronică, după cum ați văzut probabil în unele mesaje e-mail inutile care încarcă Internetul.

Problema este rezolvată prin atașarea unei semnături digitale la fișierul pe care l-ați criptat înainte de a-l trimite către destinatar. Efectuați această operație folosind tot cheia dumneavoastră secretă:

```
#pgp -sea messagefile userid
```

Vă amintiți acea frază de trecere pe care ați introdus-o când programul PGP a generat perechea dumneavoastră de chei? Aici este locul în care trebuie să o folosiți. Nu ați avut nevoie de ea pentru criptarea fișierului deoarece criptarea s-a făcut cu ajutorul cheii publice a destinatarului. Atunci când doriți să accesați cheia dumneavoastră secretă, PGP trebuie să fie sigur că este vorba de dumneavoastră, astfel că vă cere să introduceți fraza de trecere. Protejați fraza de trecere!

Utilizarea programului PGP pentru a accesa fișierele criptate

Pentru a citi un mesaj care a fost criptat cu programul PGP folosindu-se cheia dumneavoastră publică, utilizați următoarea comandă:

```
#pgp filename
```

filename este numele fișierului pe care doriți să îl citiți. Deoarece PGP trebuie să utilizeze cheia dumneavoastră secretă pentru a debloca fișierul care a fost criptat cu ajutorul cheii dumneavoastră publice, vă va invita din nou să introduceți fraza de trecere. După ce decriptează mesajul, PGP va încerca să verifice semnătura digitală (dacă există o semnătură de acest fel atașată la fișier). În acest scop, va căuta în inelul dumneavoastră cu chei cheia publică a expeditorului și o va folosi pentru a verifica semnătura.

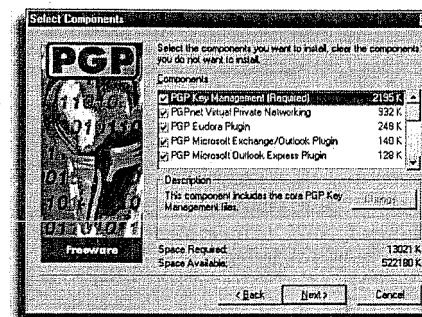
Instalarea programului PGP în Windows NT

Pentru a instala programul PGP pe un calculator cu Windows NT (sau Windows 95/98) este furnizat un program de configurare, astfel că procesul este mai simplu. Versiunea freeware este o aplicație compilată, astfel că nu este nevoie de nici un compilator C. După ce porniți programul de configurare, vă sunt prezentate licența standard și informațiile privitoare la neasumarea răspunderii, cu care trebuie să fiți de acord pentru a putea continua.

Următoarea casetă de dialog vă solicită numele dumneavoastră și al companiei. După aceasta, o altă casetă de dialog vă permite să selectați directorul care va fi folosit pentru

FIGURA 11.1

Selecția componentelor din programul PGP pe care doriți să le instalați.

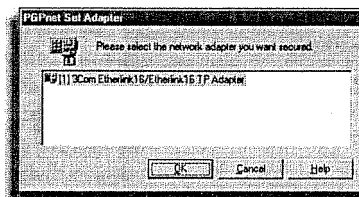


- **PGP Key Management (Gestionarea cheilor PGP)** – Aceasta este o componentă necesară și este folosită în același scop ca și fișierul inel cu chei despre care am discutat la prezentarea versiunii UNIX a programului PGP.
- **PGPnet Virtual Private Networking (Rețea privată virtuală PGPnet)** – Puteți folosi programul PGP pentru a crea o rețea privată virtuală (VPN) pentru comunicații protejate în rețeaua dumneavoastră.
- **PGP Eudora Plugin** – Dacă folosiți programul de poștă electronică Eudora, trebuie selectată această componentă.
- **PGP Microsoft Exchange/Outlook Plugin** – Dacă folosiți clientul de poștă electronică Microsoft Exchange sau Microsoft Outlook, selectați această componentă.
- **PGP Microsoft Outlook Express Plugin** – Acest program plug-in este destinat pentru a fi folosit cu Microsoft Outlook Express, o versiune redusă a programului Outlook.
- **PGP Command Line (Linie de comandă PGP)** – Selectați această componentă dacă doriți să utilizați programul PGP într-un mod linie de comandă (de obicei, poartă numele de casetă MS-DOS), similar cu versiunea UNIX.
- **PGP User's Guide (Ghidul utilizatorului PGP)** – Selectați această componentă! Este exact ceea ce spune că este!

Atunci când selectați una dintre componentele plug-in din lista precedentă, PGP adaugă elementele referitoare la securitate la meniurile clientului referit de plug-in. Aceasta înseamnă că nu trebuie să ieșiți din programul de poștă electronică pentru a cripta (sau decripta) un fișier; veți putea efectua aceste operații direct din programul client, cu ajutorul unei opțiuni de meniu.

FIGURA 11.2

Programul PGP vă invită să indicați adaptorul de rețea care va fi folosit pentru componenta VPN.



După ce ați terminat de selectat componentele, executați clic pe butonul Next; procedura de instalare va copia fișierele necesare pentru componentele pe care le-ați selectat în directorarele destinate.

Dacă ați ales să folosiți componenta PGPnet Virtual Private Networking, veți fi invitat să indicați ce adaptor de rețea veți folosi, după cum se vede în figura 11.2.

Dacă există o versiune anterioară a programului PGP instalată deja sau dacă aveți un fișier inel cu chei de la altă stație de lucru, puteți să îl folosiți cu versiunea PGP pe care tocmai ați instalat-o. Dacă doriți să folosiți această opțiune, programul de instalare vă invită să

instalare. În Figura 11.1 este prezentată caseta de dialog Select Components (Selectare componente). Această casetă de dialog este utilizată pentru alegerea componentelor pe care doriți să le instalați.

Între componentele pe care le puteți instala se numără următoarele:

specificați numele de fișier. După aceasta, programul de instalare vă va cere să încărcați din nou sistemul înainte de a începe să utilizați noua versiune de program PGP sau aplicațiile plug-in instalate.

Configurarea programului PGP în Windows NT

După ce se termină reîncărcarea sistemului, trebuie să configurați programul PGP pentru a-l putea folosi. La fel ca în versiunea UNIX, la început trebuie să creați o pereche de chei publică/secretă.

Configurarea programului PGP

1. Selectați Start, Programs, PGP și apoi PGPkeys.

FIGURA 11.3

Pentru a crea perechea de chei publică/secretă, selectați opțiunea New Key din meniul Keys.

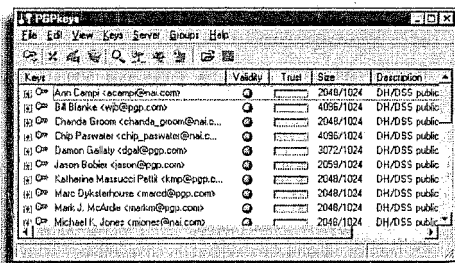


FIGURA 11.4

Când vi se cere, introduceți numele dumneavoastră și adresa de poștă electronică.

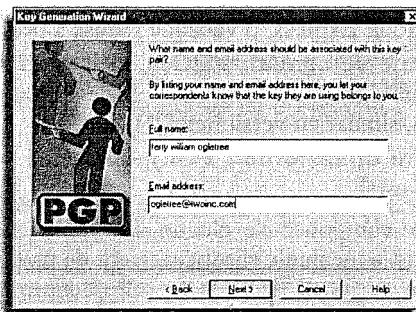
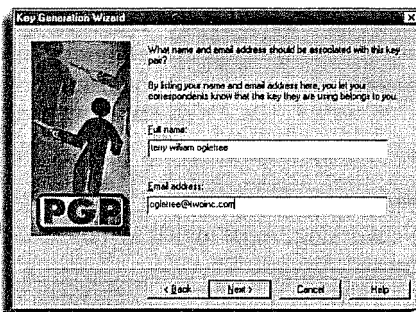


FIGURA 11.5

Selectați RSA numai dacă veți corespunde cu alte persoane care folosesc o versiune mai veche a programului PGP.



2. Din fereastra principală PGP (vezi figura 11.3), selectați opțiunea New Key (Cheie nouă) din meniul Keys (Chei).
3. După ce apare pe ecran caseta de dialog Key Generation Wizard, executați clic pe Next pentru a continua.
4. Introduceți numele dumneavoastră complet și adresa de poștă electronică în caseta de dialog care apare în continuare (vezi figura 11.4).
5. În următoarea casetă de dialog, selectați tipul de criptare pe care doriți să o folosiți, RSA sau Diffie-Hellman/DSS (vezi figura 11.5).
6. În următoarea casetă de dialog (vezi figura 11.6), selectați mărimea cheii pe care doriți să o utilizați.
7. În următoarea casetă de dialog (vezi figura 11.7), introduceți data de expirare sau executați clic pe opțiunea Key Pair Never Expires (Perechea de chei nu va expira niciodată).

FIGURA 11.6

Selectați dimensiunea cheii care trebuie generată.

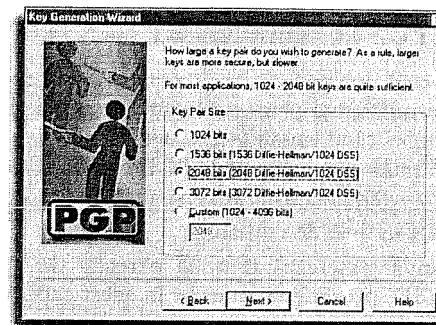


FIGURA 11.7

Selectați durata de utilizare a cheii.

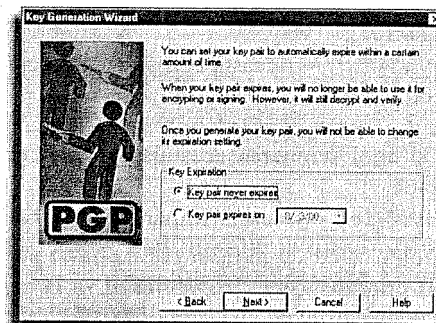
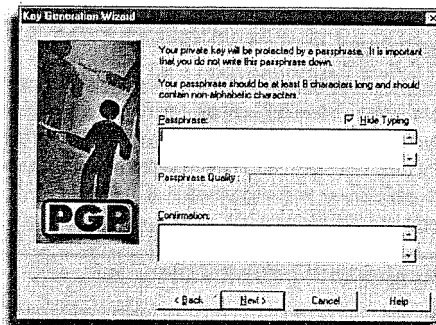


FIGURA 11.8

Fraza de trecere este folosită pentru accesul la cheia dumneavoastră secretă.



8. În final, PGP vă invită să introduceți o frază de trecere (vezi figura 11.8), care este folosită pentru protejarea cheii dumneavoastră secrete. Introduceți o frază pe care puteți să v-o amintiți și care nu este ușor de ghicit de către alte persoane.

S-ar putea să dureze câteva minute până când programul Key Generation Wizard va crea perechea dumneavoastră de chei. Aceasta depinde de viteza calculatorului dumneavoastră și de lungimea cheilor care trebuie generate. La terminare, programul wizard vă va întreba dacă doriți să trimiteți în mod automat cheia publică la un server cu chei publice din Internet. Puteți să faceți acest lucru acum sau mai târziu. De asemenea, programul wizard vă întreabă dacă doriți să faceți o copie de siguranță. Dacă acceptați, plasați copia de siguranță pe o dischetă și puneți discheta într-un loc sigur.

Ar trebui să folosiți criptarea RSA sau Diffie-Hellman/DSS?

Versiunile PGP mai vechi foloseau o metodă cunoscută ca RSA. Noile versiuni PGP (începând cu versiunea 5.0) folosesc Diffie-Hellman/DSS. Alegeți metoda de criptare pe care doriți să o folosiți bazându-vă pe versiunea utilizată de celelalte persoane cu care veți schimba mesaje. În general, ar trebui să selectați metoda mai nouă, mai puțin în cazul în care aveți foarte multe persoane de contact care folosesc o versiune PGP mai veche. Dacă vă sunt necesare ambele versiuni, puteți să generați două perechi diferite de chei, fiecare dintre ele folosind o altă formă de criptare.

Utilizarea programului PGP în Windows NT

După ce ați creat perechea de chei publică/personală, puteți folosi programul PGP pentru criptarea fișierelor. În funcție de programul plug-in selectat în etapa de instalare, ar trebui să vedeți noi elemente de meniu atunci când lansați în execuție clientul de poștă electronică. De exemplu, Microsoft Outlook are acum o intrare pentru PGP în meniul Tools (Instrumente).

Puteți să folosiți programul PGP și în linia de comandă. Comenzile sunt asemănătoare cu cele utilizate în versiunea UNIX în linie de comandă:

- `pgp -kg` – Această comandă generează o nouă pereche de chei. Vezi secțiunea „Instalarea programului PGP”, prezentată anterior în acest capitol, pentru informații privind utilizarea acestei comenzi.
- `PGP -e filename userid` – Această comandă criptează fișierul specificat prin *filename*, folosind cheia referită de *userid*.
- `pgp -s filename [-u your_userid]` – Această comandă semnează un fișier folosind cheia dumneavoastră secretă.
- `pgp -es filename userid [-u your_userid]` – Această comandă poate fi folosită pentru criptarea fișierului și apoi semnarea acestuia folosind cheia dumneavoastră secretă, într-o singură operație.
- `pgp encrypted_file [outputfile]` – Această comandă decriptează un fișier criptat.

La fel ca în versiunea UNIX, puteți să creați un fișier criptat bazat pe text ASCII în loc de un fișier binar (Blindaj ASCII) prin adăugarea parametrului `-a` la parametrul `-e` (rezultă `-ea`). Acest lucru este util în cazul în care aveți un client de poștă electronică ce nu prezintă siguranță în transferul fișierelor binare.

La ce folosesc numele dumneavoastră și adresa?

Atunci când programul Key Generation Wizard vă solicită să specificați numele și adresa de poștă electronică, nu trebuie să folosiți numele și adresa reale. Aceste informații sunt folosite pentru a face cheia dumneavoastră publică să fie recunoscută de alte persoane cărora le-o oferiți. De asemenea, aceste informații sunt utilizate când un plug-in trebuie să caute adresa dumneavoastră de poștă electronică pentru a găsi o cheie. Dacă realizați o cheie care va fi folosită într-o organizație de mai mulți utilizatori, ar trebui să introduceți aici textul care va face cheia mai ușor de identificat în cazul în care nu corespunde unei adrese de poștă electronică.

Cât ar trebui să fie valabilă o pereche de chei?

Atunci când creați o pereche de chei, puteți cere programului PGP să creeze o pereche de chei care să nu expire niciodată. Aceasta poate fi o alegere bună dacă realizați o singură pereche de chei pentru dumneavoastră, pe care intenționați să o folosiți o perioadă îndepărtată. Însă dacă lucrați la un proiect special care se va derula numai pe o perioadă limitată de timp, puteți stabili pentru o cheie o dată de expirare. După data de expirare, cheia nu va mai putea fi folosită pentru criptarea fișierelor.

Rezumat

PGP este un instrument util, în special pentru poșta electronică. Vă permite să criptați textele sau alte fișiere înainte de expedierea acestora prin rețea (sau prin Internet). De asemenea, programul PGP poate folosi semnături digitale pentru a vă ajuta să oferiți o garanție destinatarului că fișierul a fost generat chiar de dumneavoastră.

Partea a III-a

Instalarea și configurarea firewall-urilor

Capitolul 12 • Instrumente pentru firewall-uri disponibile în Internet	198
Capitolul 13 • Utilizarea produsului TCP Wrappers	208
Capitolul 14 • Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)	217
Capitolul 15 • SOCKS	241
Capitolul 16 • SQUID	249
Capitolul 17 • Utilizarea programelor <i>ipfwadm</i> și <i>ipchains</i> sub Linux	258
Capitolul 18 • Microsoft Proxy Server	272
Capitolul 19 • Firewall-ul Elron CommandView	288
Capitolul 20 • Dispozitive firewall	299
Capitolul 21 • Firewall-uri și mai mult decât atât	306

Instrumente pentru firewall-uri disponibile în Internet

- Utilizarea produselor freeware și shareware
- TCP Wrappers
- Setul de instrumente FWTk (TIS Firewall Toolkit)
- SOCKS
- SQUID
- Drawbridge
- SATAN
- Alte programe de securitate utile

Utilizarea produselor freeware și shareware

Aproape zilnic apar noi producători de firewall-uri. Dacă aș vrea să fac o listă a tuturor celor care oferă în prezent produse pe această piață, aș umple jumătate din carte. Din nefericire, în momentul în care această carte va fi tipărită și distribuită în librării, unii dintre acești producători vor fi dispăruți, în timp în cursă vor fi intrat alții.

Atunci când începeți să vă gândiți la modul în care vreți să implementați un firewall, unul dintre lucrurile pe care le aveți de făcut este să evaluați produsele disponibile și să determinați cum se integrează acestea în arhitectura pe care o proiectați pentru firewall. Unii furnizori oferă servicii complete, punându-vă la dispoziție tot ce aveți nevoie, inclusiv filtrarea pachetelor, servere intermediar pentru aplicații, alte produse software de securitate și chiar instruire și asistență tehnică permanentă. Dacă nu aveți personal experimentat pentru întreținerea unui firewall, puteți alege această cale.

Totuși, înainte de a alege o anumită soluție, ar trebui să citiți până la capăt acest capitol pentru a vă informa cu privire la câteva dintre firewall-urile ce pot fi descărcate din Internet. Cele mai multe dintre acestea sunt gratuite sau sunt puse la dispoziție în schimbul unei mici sume. Unele, cum ar fi TIS Firewall Toolkit, pot fi descărcate gratuit, dar au o „rudă” pe care o puteți cumpăra – o versiune comercială ce include mai multe caracteristici decât versiunea gratuită.

Chiar dacă decideți să nu folosiți nici unul dintre aceste produse în firewall-ul dumneavoastră, simpla înțelegere a modului lor de funcționare vă poate ajuta să faceți o alegere

mai bună atunci când va veni timpul să evaluați produsele pentru care va trebui să plătiți. În acest capitol vor fi prezentate pe scurt câteva dintre cele mai populare produse. În capitolele care urmează veți afla mai multe detalii despre unele dintre aceste produse.

TCP Wrappers

Acest set de programe a fost creat de Wietse Venema pentru a crește securitatea rețelei Universității Tehnologice Eindhoven, unde era angajat în perioada respectivă. Scopul acestui program container este de încorpora un strat pentru conectare și controlul accesului în modelul serviciilor de rețea TCP/IP de tip client/server.

TCP Wrappers folosește un proces demon, numit `tcpd`, lansat în locul serviciilor de rețea definite în fișierul `inetd.conf`. În configurația obișnuită, Internet Daemon (`inetd`) ascultă cererile de servicii de rețea recepționate, apoi determină serviciul necesar comparând numărul de port din cerere cu serviciile definite în fișierul `/etc/services`. Folosind numele serviciului, `inetd` folosește apoi informațiile de configurare din fișierul `inetd.conf` pentru a determina ce protocol să folosească și cum să lanseze procesul demon necesar.

Vezi și

- Pentru mai multe informații despre modul de folosire a porturilor de către protocoalele TCP și UDP, vezi pagina 46.
- Pentru o listă a porturilor TCP și UDP recunoscute, vezi pagina 318.

Problema acestui scenariu este faptul că nu asigură controlul accesului. Câteva dintre serviciile pe care le lansează, cum ar fi FTP și Telnet, implementează propriile metode pentru controlul accesului, cerând introducerea unui nume de utilizator și a unei parole. Totuși, această metodă nu este suficientă pentru protejarea completă a sistemului și a rețelei din care face parte acesta. De ce? Deoarece aceste utilitare, ca și altele, transmit numele de utilizator și parola sub formă de text clar, care poate fi interceptat chiar și de un hacker cu cunoștințe medii. Nu există un control bazat pe gazda de la care provin numele de utilizator și parola. Nu există nici o metodă care să poată fi folosită pentru a permite accesul numai de la gazdele de rețea și adresele pe care le cunoașteți și cărora le puteți acorda o oarecare încredere.

TCP Wrappers asigură această posibilitate. În plus, suplinește și o altă deficiență a demonului `inetd`: TCP Wrappers prevede înregistrarea cererii de servicii și a gazdei care a făcut cererea. Această informație poate fi foarte valoroasă atunci când încercați să determinați dacă a avut loc o pătrundere în rețea.

Pentru folosirea produsului TCP Wrappers, mai întâi descărcați codul sursă și îl compilați pe sistemul dumneavoastră. Instrucțiunile de compilare pentru cele mai populare variante UNIX sunt incluse în documentația care însoțește codul sursă. După ce compilați programul, puteți să editați câteva fișiere pentru a configura utilizarea programului:

- `inetd.conf` – În acest fișier înlocuiți cu programul demon `tcpd` programul de deservire pe care îl apelează în mod obișnuit `inetd` pentru a răspunde la o anumită cerere de servicii. Programul de deservire este transmis ca argument demonului `tcpd`, care determină dacă este permis accesul, asigură înregistrarea cererii și lansează demonul de deservire corespunzător.

■ **hosts.allow** – Acesta nu este un fișier de configurare UNIX obișnuit, ci este specific programului TCP Wrappers. În acest fișier creați un set de reguli folosite pentru a determina la ce servicii are acces fiecare gazdă. Pentru controlul accesului, în acest fișier puteți folosi nume de gazde, nume de domenii sau adrese IP. De asemenea, puteți executa comenzi de nucleu în funcție de servicii și de gazde.

■ **hosts.deny** – Acesta este perechea fișierului **hosts.allow** și este folosit în scopul opus. Aici creați reguli pentru a interzice accesul unor anumite gazde, domenii sau adrese IP.

Demonul TCP Wrappers folosește demonul **syslogd** pentru înregistrare și trimite datele de înregistrare în același loc ca și demonul **sendmail**. Puteți configura modul de operare al demonului **syslogd** prin editarea fișierului **syslogd.conf**.

Vezi și

➤ Pentru mai multe informații despre demonul **syslogd** și despre fișierul de configurare **syslogd.conf**, vezi pagina 151.

TCP Wrappers este un utilitar foarte popular. Este inclus în unele implementări UNIX și Linux. Deși nu este în sine o soluție completă pentru un firewall, poate fi folosit ca măsură suplimentară de securitate pentru orice gazdă care oferă servicii în rețea.

Pachetul TCP Wrappers poate fi descărcat de pe următorul sit:

<ftp://ftp.porcupine.org/pub/security/>

Capitolul 13, „Utilizarea produsului TCP Wrappers“ prezintă mai multe detalii despre acest utilitar, arătându-vă cum să editați fișierul **inetd.conf** și cum să creați regulile pentru fișierele **hosts.allow** și **hosts.deny**.

Setul de instrumente TIS Firewall Toolkit

Trusted Information Systems Internet Firewall Toolkit – de obicei numit FWTK sau The Toolkit – există de ceva timp. Atunci când Trusted Information Systems (TIS) a fuzionat cu Network Associates, noua companie era și furnizoarea firewall-ului Gauntlet. Deși Gauntlet a fost proiectat inițial ca o versiune comercială a setului FWTK, de atunci a fost dezvoltat și îmbunătățit, așa că, în cea mai mare parte, conține cod diferit față de setul de instrumente FWTK.

Deoarece FWTK a fost dezvoltat pentru agenția DARPA (Defense Advanced Research Projects Agency), codul a fost plasat în domeniul public. Puteți să îl descărcați din Internet, după ce vă declarați de acord cu termenii licenței. Acest lucru se face trimițând o solicitare prin e-mail către TIS. Ca răspuns, primiți, de obicei după doar câteva minute, un mesaj e-mail automatizat, care vă comunică numele unui director temporar (disponibil numai 12 ore) din care puteți să descărcați programele prin FTP.

Ca și TCP Wrappers, setul FWTK este furnizat în cod sursă, scris în limbajul de programare C. Înainte de a-l putea folosi trebuie să îl compilați pe sistemul dumneavoastră. În timp ce TCP Wrappers nu face decât să adauge controlul accesului și funcții de înregistrare în jurnal la servicii deja existente pe server, componentele oferite de setul FWTK sunt aplicații intermediar reale. Aceasta înseamnă că, dacă sunt configurate corect pe o gazdă

bastion întărită, aplicațiile intermediar permit folosirea serviciilor de rețea prin firewall, fără să permită transferul direct al pachetelor IP între rețeaua locală protejată și exterior.

Vezi și

➤ „Utilizarea gazdelor bastion și a gazdelor de sacrificiu“, în Capitolul 4, la pagina 90.

➤ „Utilizarea unei gazde bastion“, la pagina 112.

➤ „Utilizarea unei porți intermediare de aplicații“, la pagina 83.

➤ „Porți de aplicații și servere intermediar“, la pagina 132.

Componentele importante ale setului FWTK sunt aplicații intermediar folosite pentru cele mai populare utilitare TCP/IP. Instrumentele software incluse în pachet sunt următoarele:

- **netac1** – Aplicație pentru Telnet, Finger și liste pentru controlul accesului în rețea.
- **smap** și **smagd** – Aplicații pentru un serviciu SMTP sigur.
- **ftp-gw** – Aplicație pentru un server intermediar pentru FTP.
- **tn-gw** – Aplicație pentru un server intermediar pentru Telnet.
- **rlogin-gw** – Aplicație pentru un server intermediar pentru Rlogin.
- **plug-gw** – Aplicație pentru un serviciu intermediar cu scop generic.
- **authd** – Aplicație pentru un serviciu de autentificare, cu scopul de a îmbunătăți practicile de „autentificare puternică“.
- **telnetd** – Un server Telnet care poate fi folosit pentru gestionarea firewall-ului.
- **login-sh** – Un program de conectare îmbunătățit, care asigură suportul pentru conectările sigure ce folosesc chei hardware de autentificare (token), cum ar fi o cartelă inteligentă (smart card).
- **syslogd** – O aplicație care înlocuiește demonul de înregistrare UNIX tradițional.

Componenta **netac1** este configurată de obicei pentru a asigura accesul serviciilor la firewall-ul propriu-zis, în timp ce alte aplicații intermediar – cum ar fi **tn-gw** și **ftp-gw** – sunt folosite pentru a asigura intermedierea prin firewall. Acestea permit utilizatorilor externi să obțină acces la servicii aflate pe gazde din rețeaua locală, și invers.

Vezi și

➤ În capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)“, veți găsi mai multe detalii despre modul de funcționare a setului de instrumente și despre configurarea serviciilor intermediar pentru rularea pe un sistem UNIX.

SOCKS

SOCKS este un protocol destinat funcționării într-un mediu client/server. Un server SOCKS rulează pe o gazdă firewall și asigură un serviciu de intermediere. Atunci când un client din afara rețelei locale protejate dorește să se conecteze la un anumit serviciu, o face direct, dacă este disponibilă o conexiune directă. Dacă nu, încearcă să ia legătura cu serverul intermediar SOCKS și, schimbând mesaje definite de protocolul SOCKS, negociază o conexiune intermediată. După stabilirea unei conexiuni, clientul comunică cu

serverul SOCKS folosind protocolul SOCKS. Serverul de aplicații comunică cu serverul SOCKS ca și cum acesta ar fi clientul propriu-zis.

În acest moment există două versiuni ale protocolului SOCKS. Versiunea 4 este distribuită pe scară largă și asigură compatibilitatea cu aplicațiile bazate pe TCP. Versiunea 5, descrisă în câteva documente Request For Comments, adaugă suportul pentru aplicațiile UDP și autentificarea.

Vezi și

- „Protocolul de control al transmisiei (TCP)“, la pagina 32.
- „Protocolul UDP (User Datagram Protocol)“, la pagina 32.

Spre deosebire de serviciile intermediar asigurate de TIS Firewall Toolkit, clienții care folosesc protocolul intermediar SOCKS trebuie să fie mai întâi adaptați pentru acesta. De obicei, aceasta înseamnă recompilarea clienților pentru adăugarea în cod a funcțiilor client SOCKS. Există câteva excepții de la această regulă. Furnizorii au dezvoltat biblioteci pentru clienți Windows, care permit programelor client existente să folosească protocolul SOCKS. De asemenea, protocolul SOCKS a fost adoptat de un număr mare de producători de software care au asigurat produselor client proprii funcții SOCKS. În plus, implementarea SOCKS versiunea 4, pusă la dispoziție de NEC, include clienți pentru Telnet, FTP, Finger și WHOIS. Pachetul SOCKS versiunea 5 adaugă clienți pentru Archie, PING și traceroute.

Vezi și

- *Deoarece este o soluție atât de populară pentru un server intermediar, protocolului SOCKS îi este dedicat un capitol întreg. Vezi capitolul 14, „SOCKS“, pentru mai multe informații despre modul de funcționare a protocolului și pentru surse de aplicații client și biblioteci SOCKS.*

SQUID

SQUID este numele unui server de cache intermediar, disponibil în Internet. Ca și setul TIS Firewall și alte câteva instrumente populare despre care am discutat în acest capitol, SQUID este disponibil sub formă de cod sursă și poate fi compilat sub multe variante populare de UNIX.

Un server intermediar, așa cum am arătat, funcționează prin interceptarea traficului IP dintre client și server. Serverul intermediar comunică cu fiecare dintre cele două sisteme, îndeplinind rolul unui mesager, astfel încât între cele două sisteme nu se face niciodată un schimb direct de pachete IP. Serverele intermediar pot ascunde identitatea clienților aflați dincolo de firewall. Un server de cache are o funcție total diferită. Utilizarea cache-ului constă în păstrarea unor copii ale obiectelor intens solicitate, astfel încât atunci când apare o nouă cerere pentru unul dintre aceste obiecte, răspunsul să fie dat din cache. Prin deservirea cererilor din cache, de obicei clienții primesc răspunsurile mai repede decât în cazul interogării directe a sursei obiectului.

Obiectele pe care serverul de cache le păstrează în memorie (sau în fișiere de pe disc) includ date primite ca răspuns la cereri transmise prin FTP, HTTP și alți clienți de rețea. Pe lângă aceste obiecte, SQUID permite și păstrarea în cache a căutărilor DNS. SQUID este

compus din mai multe programe, inclusiv un server de cache intermediar (numit squid), un program de căutare DNS, numit dnsserver, și alte aplicații opționale.

SQUID este compatibil cu protocolul Lightweight Internet Cache

Un server de cache stochează pentru o anumită perioadă de timp datele pe care le-a obținut pentru un client, astfel încât să poată răspunde mai repede dacă se face o altă cerere pentru aceleași date. Serverele de cache folosesc protocolul HTTP, de exemplu, pentru a obține paginile Web care sunt apoi transmise clienților serverului. Totuși, serverele de cache pot să schimbe date și între ele. Protocolul folosit în acest scop se numește Lightweight Internet Cache Protocol, sau ICP.

Protocolul ICP este descris de două documente RFC: RFC 2186, „Internet Cache Protocol (ICP), Version 2“, și RFC 2187, „Application of Internet Cache Protocol (ICP), Version 2“.

Vezi și

- Capitolul 7, „Porți de aplicații și servere intermediar“, la pagina 132.
- Capitolul 18, „Microsoft Proxy Server“, la pagina 272.
- Capitolul 16, „SQUID“, la pagina 249.

Serverele SQUID pot fi configurate într-o manieră ierarhică, cu serverele părinte aflate cel mai aproape de coloana vertebrală Internet și cu serverele descendent localizate mai aproape de utilizatorii din rețeaua internă. Atunci când un server descendent nu poate rezolva o cerere folosind datele din cache-ul propriu, trimite o interogare către serverul părinte. Serverul părinte rezolvă cererea din cache-ul propriu sau face o altă cerere către următorul server din ierarhie. Folosirea acestei organizări ierarhice vă poate ajuta să economisiți lărgime de bandă prețioasă, deoarece cererile pot fi uneori rezolvate local, fără apelarea unui singur server care trebuie să rezolve cererea din resursele proprii sau să facă o cerere prin Internet. SQUID folosește protocolul ICP (Lightweight Internet Cache Protocol) pentru comunicațiile dintre serverele părinte și serverele descendent.

Un avantaj pe care SQUID îl are față de unele dintre produsele despre care am discutat este faptul că asistența tehnică poate fi obținută nu numai din pagini Web, liste poștale și alte resurse din Internet, ci și de la furnizori, care, în schimbul unei anumite taxe, vă pot ajuta să implementați produsele și asigura asistența tehnică.

Pentru configurarea serverului SQUID, trebuie să editați un fișier numit squid.conf. De asemenea, SQUID produce câteva fișiere jurnal, care includ informații de acces și informații despre performanțele cache-ului.

Vezi și

- *Și în acest caz, deoarece acest produs software este folosit pe o scară atât de largă, un întreg capitol prezintă detalii despre instalare și configurare. Pentru mai multe informații, vezi capitolul 16, „SQUID“.*

Drawbridge

Până acum în acest capitol, am prezentat produse care funcționează, în esență, ca servere intermediar. Rețineți, totuși, că pentru o funcționare optimă, serverul intermediar ar trebui să fie plasat în spatele unui filtru de pachete, nu să fie conectat direct la Internet. Ca filtru

de pachete puteți folosi un ruter cu ecranare (screening router) sau un program software rulat pe un calculator gazdă.

Drawbridge este un filtru de pachete cu viteză mare, disponibil gratuit. Deși inițial rula pe platforme DOS, acum rulează pe platforme FreeBSD UNIX. Ca și Drawbridge, FreeBSD este disponibil gratuit – de unde și numele! Această aplicație de filtrare a pachetelor a fost dezvoltată la Universitatea A&M din Texas și a fost proiectată ținându-se seama de mediul academic.

Vezi și

- „Utilizarea unui filtru de pachete“, în Capitolul 4, la pagina 81.
- „Filtrarea pachetelor“, la pagina 95.

Pentru instalarea aplicației Drawbridge, ar trebui să instalați mai întâi sistemul de operare FreeBSD, deoarece Drawbridge modifică unele fișiere din directorul /etc. De asemenea, este o idee bună, la fel ca pentru orice gazdă bastion, să folosiți sistemul respectiv numai pentru filtrarea pachetelor și să nu îl încărcați cu o mulțime de conturi de utilizator și alte aplicații.

Drawbridge este format din trei componente de bază:

- **Motorul de filtrare Drawbridge** Această componentă execută munca propriu-zisă de filtrare a pachetelor și este compilată în nucleul sistemului de operare.
- **Compilatorul de filtrare Drawbridge** Aceasta este o aplicație la nivelul utilizatorului, folosită pentru compilarea regulilor pe care le plasați în fișierul de configurare, astfel încât acestea să poată fi folosite de motorul de filtrare. Acest program se numește dbfc.
- **Gestionarul Drawbridge** Evident, aceasta este aplicația de gestionare pe care o folosiți pentru controlul programului Drawbridge. Această aplicație se numește dbmgr.

Configurarea filtrului se face prin crearea unui fișier de text cu reguli bazate pe comenzile acceptate de programul Drawbridge, urmată de compilarea și încărcarea filtrului. Fișierul de configurare este creat folosind orice editor de texte și este compilat cu ajutorul comenzii dbfc:

```
dbfc input-file [output-file]
```

După ce produceți fișierul de ieșire compilat, puteți folosi comanda dbmgr pentru încărcarea filtrului.

Ce este FreeBSD?

FreeBSD este un sistem de operare bazat pe sistemul de operare BSD UNIX și este scris pentru a fi rulat pe calculatoarele compatibile PC. Pentru cei care nu își pot permite o stație de lucru SPARC performantă sau un calculator HP UNIX, FreeBSD este o alternativă bună. FreeBSD și documentația care îl însoțește sunt întreținute de numeroase persoane care, de-a lungul anilor, au consumat timp și energie pentru dezvoltarea unui sistem de operare ce rivalizează cu cele „cumpărate“.

Pentru mai multe informații despre FreeBSD sau pentru descărcarea codului, a documentației și a altor fișiere asociate cu acestea, vizitați situl Web: www.freebsd.org.

Filtrele pe care le creați pot fi folosite pentru a permite sau a bloca accesul, în funcție de un serviciu de rețea (definit în fișierul /etc/services), o valoare numerică a unui port sau un tip numeric ICMP. De asemenea, filtrarea se poate face în funcție de portul sursă sau

destinație ori de protocolul folosit (TCP, UDP sau ICMP). La fel ca în cazul celor mai multe filtre bune de pachete, puteți defini regulile de filtrare în funcție de direcția traficului (către interior sau către exterior), de adresa IP sau de numele de gazdă.

Deoarece Drawbridge nu este un produs comercial, nu este disponibilă asistență prin Internet. De asemenea, trebuie să aveți cunoștințe aprofundate despre gestionarea sistemelor UNIX (preferabil FreeBSD) și lucrul în rețele TCP/IP.

Pentru mai multe informații despre Drawbridge sau pentru descărcarea documentației și a pachetului propriu-zis, vizitați situl Web Drawbridge:

drawbridge.tamu.edu/

SATAN

Având un nume atât de nefast, ați putea să vă gândiți că utilitarul SATAN este instrumentul potrivit pentru un hacker care vrea să vă distrugă rețeaua. De fapt, termenul este acronimul pentru System Administrator's Tool for Analyzing Network (Instrumentul administratorului de sistem pentru analiza rețelei). Dacă numele vă displace, utilitarul vă pune la dispoziție o opțiune prin care puteți schimba în SANTA numele afișat pe ecran. Indiferent de nume, acest instrument folosește tehnici pasive pentru căutarea eventualelor probleme de securitate din rețeaua dumneavoastră. În realitate, SATAN nu este un server intermediar, un filtru de pachete sau o altă componentă a unui firewall. Este menționat în acest capitol deoarece este unul dintre cele mai importante instrumente care, folosite corect, vă pot ajuta să determinați dacă firewall-ul dumneavoastră face ceea ce vă așteptați. SATAN este furnizat, ca și celelalte aplicații descrise în acest capitol, sub formă de cod sursă și poate fi compilat pe multe sisteme UNIX. Este folosit, în principal, pentru investigarea gazdelor UNIX.

Atunci când folosiți utilitarul SATAN, puteți opta pentru o scanare superficială sau dură. Pe sistemele țintă sunt executate o diversitate de verificări, în special pentru porturile folosite de multe servicii de rețea populare, cum ar fi FTP, HTTP, NFS, NIS, Remote Shell Access, sendmail și așa mai departe.

„Cum să îmbunătățiți securitatea sitului dumneavoastră prin pătrundere forțată“

Acesta este titlul unui articol scris de Dan Farmer și Wietse Venema, autorii utilitarului SATAN. Acest articol discută câteva dintre metodele obișnuite de pătrundere în rețele și merită să fie citit dacă faceți primii pași în domeniul securității rețelelor. Poate fi găsit în mai multe locuri din Internet, inclusiv la următoarea adresă:

<http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking-101.html>

După ce descărcați codul SATAN și decompriți fișierul, obțineți o serie de subdirectoare grupate sub un director numit /rules. Aceste subdirectoare sunt folosite după cum urmează:

- /facts – Aceste reguli sunt folosite pentru deducerea noilor informații pe baza datelor colectate de SATAN.

¹ „Improving the Security of your Site by Breaking Into It“ (n. trad.)

- **Hosttype** – Aceste reguli sunt folosite de SATAN pentru a determina tipul gazdei. Acest lucru este realizat prin examinarea mesajelor de prezentare afișate de sistemul de operare sau de utilitare precum FTP ori sendmail.
- **/services** – Aceste reguli sunt folosite de SATAN pentru a determina ce tip de gazdă examinează, în funcție de serviciile pe care le găsește – client sau server.
- **/todo** – Aceste reguli sunt folosite pentru a decide ce va face SATAN în continuare, în funcție de scanările efectuate deja pe anumite gazde.
- **/trusts** – SATAN decide care sunt tipurile de gazde cărora le acordă încredere sistemul investigat.
- **/drop** – Aceste reguli îi spun programului SATAN ce informații să ignore. În prezent, aici este inclusă o singură regulă, conform căreia SATAN ignoră directoarele de pe CD-ROM exportate de NFS.

De asemenea, există alte directoare în care sunt păstrate rutine PERL, documentație și programe executabile.

Dacă urmează să folosiți acest instrument pentru investigarea problemelor de securitate din rețeaua dumneavoastră, aveți nevoie de ceva timp pentru citirea documentației și configurarea regulilor. Acest instrument nu este destinat persoanelor neexperimentate, ci celor care au cunoștințe aprofundate despre sistemul de operare UNIX și TCP/IP. Deși configurarea programului SATAN poate consuma mult timp, folosirea periodică a acestuia și actualizarea cu noi versiuni vă pot ajuta să îmbunătățiți securitatea rețelei dumneavoastră. Programul automatizează multe procese pe care, altfel, ar trebui să le executați manual și produce rapoarte prin care rezumă ceea ce găsește.

Dacă vreți să înțelegeți mai bine acest instrument, fără să vă bateți capul cu descărcarea și instalarea întregului pachet, vizitați următorul sit Web:

http://www.am.qub.ac.uk/world/documentation/satan_doc/html/docs/satan_reference.html

Situl de la această adresă URL indică un fișier de referință pentru SATAN și descrie, până la un anumit nivel, întregul produs, inclusiv fișierele de configurare, regulile și așa mai departe.

SATAN este un utilitar extensibil

Deoarece problemele de securitate se schimbă rapid în Internet, unele instrumente se învechesc repede, pe măsură ce sunt descoperite noi puncte vulnerabile. Totuși, SATAN este un utilitar extensibil și poate fi adaptat pentru noi evenimente în acest mediu aflat într-o continuă schimbare. Puteți adăuga în utilitar noi tipuri de teste, configurând regulile care le guvernează funcționarea. Dacă vă familiarizați cu documentația utilitarului SATAN și aveți unele cunoștințe de programare în C, acest utilitar poate avea o viață lungă.

Alte programe de securitate utile

Acest capitol a prezentat pe scurt câteva dintre instrumentele pe care puteți să le descărcați din Internet și să le folosiți pentru construirea unui firewall. De asemenea, am discutat pe scurt despre SATAN, ca instrument de raportare a problemelor de securitate. Deși subiectul principal al acestei cărți îl reprezintă firewall-urile, este important pentru

dumneavoastră să puteți monitoriza rețeaua, astfel încât să vă asigurați că firewall-ul vă protejează împotriva metodelor cunoscute de atac.

În anexa B, „Alte instrumente de securitate pe care le puteți folosi“, veți găsi un ghid ce descrie o serie de instrumente bune – unele sunt noi, altele sunt testate și verificate în practică de mai mulți ani. Cele mai multe dintre instrumentele menționate în anexă pot fi descărcate gratuit de pe situri din Internet. Nu uitați că și hackerii pe care încercați să îi opriți cunosc aceste instrumente și ar putea să le folosească pentru a obține informații despre rețeaua dumneavoastră. Ar fi bine să citiți această anexă și, când aveți timp, să studiați unele dintre instrumentele descrise aici.

Rezumat

Firewall-urile sunt produse ce pot fi cumpărate – unele la un preț destul de mic, altele pentru sume astronomice. În multe cazuri, primiți ceea ce ați plătit. Totuși, ținând seama că din Internet pot fi descărcate gratuit atât de multe componente pentru firewall-uri, ar trebui să luați în considerare posibilitatea de a le studia, pentru a ști ce să așteptați de la un produs comercial. Dacă aveți cunoștințele necesare pentru administrarea sistemelor UNIX și TCP/IP, s-ar putea să descoperiți că instrumentele gratuite vă sunt suficiente.

În următoarele capitole veți găsi mai multe detalii despre câteva dintre aceste instrumente.

Capitolul 13

Utilizarea produsului TCP Wrappers

- Prezentarea produsului TCP Wrappers
- Obținerea produsului TCP Wrappers
- Configurarea produsului TCP Wrappers
- Limitele produsului TCP Wrappers

Prezentarea produsului TCP Wrappers

Protocoloalele TCP/IP de bază au fost dezvoltate cu mai mulți ani în urmă pentru a permite legarea rețelelor de diferite tipuri. Cele mai multe dintre sistemele care au implementat inițial протокоalele TCP/IP erau situri academice și guvernamentale, iar în momentul respectiv cerințele de securitate ale acestei comunități de utilizatori nu semănau deloc cu situația actuală. Într-adevăr, протокоalele TCP (Transmission Control Protocol), IP (Internet Protocol) și UDP (User Datagram Protocol) nu au fost dezvoltate având securitatea ca unul dintre scopurile principale. Era suficient dacă aceste протокоale permiteau diferitelor sisteme de calcul brevetate să schimbe date între ele. Utilitățile care au urmat, cum ar fi Telnet și FTP, moștenesc aceeași caracteristică. Telnet și FTP, de exemplu, impun ca măsură de securitate transmiterea unui nume de utilizator și a unei parole valabile pentru sistemul țintă. Mecanismul de securitate pierde din importanță atunci când vă dați seama că numele de utilizator și parola sunt transmise în rețea sub formă de text clar, care poate fi interceptat de cineva care are un anumit nivel de cunoștințe.

La începutul anilor '80, când calculatoarele personale au început să pătrundă în mediile de afaceri, au fost dezvoltate multe протокоale de rețea diferite de către producători care încercau să obțină profituri pe noua piață. Novell Netware exista deja într-o formă de început și a câștigat rapid o parte din piață. Totuși, pe măsură ce sistemul de operare UNIX a fost adoptat pe scară din ce în ce mai largă, протоколul TCP/IP a devenit tot mai popular. O dată cu dezvoltarea explozivă a Internetului, TCP/IP a devenit, pentru toate scopurile practice, suita prestabilită de протокоale de rețea și a fost adoptată de toți furnizorii importanți de calculatoare și software de rețea.

Există multe produse ce pot fi folosite pentru a îmbunătăți securitatea rețelei dumneavoastră, cum ar fi firewall-urile – subiectul acestei cărți. Un firewall este format din mai multe componente, iar TCP Wrappers poate fi una dintre acestea. Deși filtrul de pachete poate fi un început bun pentru un firewall, el nu poate intercepta totul.

TCP Wrappers a fost dezvoltat de Wietse Venema la Universitatea Tehnologică Eindhoven pentru a contribui la protejarea calculatoarelor din universitate împotriva atacurilor. TCP Wrappers restricționează serviciile de rețea ce pot fi folosite, precum și gazdele cărora li se permite să le folosească. TCP Wrappers poate fi configurat pentru manipularea celor mai multe dintre serviciile de bază pe care le găsiți de obicei pe un sistem UNIX, cum ar fi:

- Telnet
- Finger
- FTP
- Exec
- RSH
- Rlogin
- TFTP

Principala caracteristică pe care o au în comun aceste servicii este faptul că există o mapare biunivocă între numele serviciului și un program executabil care asigură serviciul.

Cum funcționează programul TCP Wrappers

Atunci când programul demon `inetd` primește o cerere de rețea, determină ce serviciu trebuie să lanseze, în funcție de numărul portului. Fișierul `/etc/services` conține o mapare între numele serviciilor și numerele porturilor. După ce determină serviciul ce trebuie lansat, `inetd` citește fișierul de configurare (`inetd.conf`) pentru a descoperi ce program ar trebui să ruleze pentru a rezolva cererea.

Vezi și

- Pentru mai multe informații despre modul în care sunt folosite numerele de porturi de către протокоalele TCP și UDP, vezi capitolul 2, „Introducere în suita de протокоale TCP/IP”, la pagina 26.
- Pentru o listă a porturilor TCP și UDP recunoscute, vezi anexa A, „Porturi uzuale TCP și UDP”, la pagina 317.

Pentru ca demonul TCP Wrappers (`tcpd`) să ia decizii de control al accesului și să își îndeplinească sarcinile de înregistrare în jurnale, trebuie să editați fișierul `inetd.conf` pentru a preciza că este rulat demonul `tcpd` în locul programului executabil care răspunde în mod normal cererii de serviciu. Demonul `tcpd` își îndeplinește sarcinile și, dacă gazda care a făcut cererea are dreptul să folosească serviciul, lansează programul executabil pentru serviciul respectiv. Ca urmare, TCP Wrappers se inserează între demonul `inetd` și serviciul de rețea.

Conectarea prin `syslogd`

TCP Wrappers asigură nu doar controlul accesului pentru serviciile împreună cu care este folosit, ci și înregistrarea în jurnale, astfel încât să puteți determina cine folosește serviciile. Informațiile care trebuie înregistrate în jurnal sunt transmise către demonul `syslogd`, care asigură și posibilitatea de înregistrare centralizată pentru multe componente ale sistemului de operare UNIX. În mod prestabilit, TCP Wrappers trimite informațiile de înregistrare în

jurnal în același loc ca și jurnalele de tranzacții ale demonului sendmail. În general, syslogd poate transmite informațiile de jurnal către unul sau mai multe fișiere, către consola de sistem, către o consolă de utilizator sau către un utilizator, printr-un mesaj e-mail. Modul în care syslogd stabilește ce să facă cu informațiile de jurnal este controlat prin datele din fișierul de configurare, numit, de obicei, /etc/syslog.conf.

Vezi și

➤ Pentru mai multe informații despre syslogd și fișierul de configurare syslogd.conf, vezi capitolul 8, „Tehnici de monitorizare și auditare a sistemului de operare”, la pagina 148.

Obținerea produsului TCP Wrappers

S-ar putea să aveți deja utilitarele TCP Wrappers. Acesta este un set de programe atât de popular, încât este livrat ca parte a unor versiuni UNIX și Linux. Dacă nu le aveți în sistem, le puteți găsi în multe locuri din Internet. Puteți folosi următoarea adresă URL pentru a obține pachetul TCP Wrappers prin FTP, împreună cu alte instrumente utile dezvoltate de Wietse Venema, cum ar fi utilitarul SATAN:

ftp://ftp.porcupine.org/pub/security/

Utilitarele TCP Wrappers sunt disponibile, de obicei, sub formă de cod sursă și așa ceva veți găsi în acest sit. După descărcarea fișierelor, nu uitați să verificați fișierul readme pentru a afla informații despre eventualele actualizări sau despre modul de compilare a codului sursă pe sistemul dumneavoastră.

Unde puteți găsi programele TCP Wrappers?

Multe îndrumare și alte documente pe care le veți găsi în Web indică locuri din care puteți descărca programele TCP Wrappers. Totuși, rețineți că în multe dintre aceste locuri nu se mai află codul programelor. Adresa URL indicată în această secțiune (porcupine.org) este adresa oficială a utilităților scrise de Wietse Venema.

Configurarea produsului TCP Wrappers

Pentru folosirea utilităților TCP Wrappers pe un sistem UNIX, mai întâi compilați codul sursă (conform instrucțiunilor din documentația specifică variantei de UNIX pe care o aveți). După ce obțineți programul executabil tcpd, puteți edita fișierele de configurare care controlează modul de folosire a acestuia. Aceste fișiere sunt următoarele:

- **inetd.conf** – Editați acest fișier pentru a insera referințe la demonul tcpd în înregistrările corespunzătoare serviciilor pe care vreți să le încapsulați în utilitarele TCP Wrappers.
- **hosts.allow** – Acest fișier conține regulile care definesc cui îi este permis să folosească fiecare serviciu lansat de tcpd.
- **hosts.deny** – Acest fișier conține regulile care definesc cui îi este interzis explicit accesul la fiecare serviciu lansat de tcpd. Acest fișier este citit ultimul, așa că, dacă în fișierul hosts.allow este găsită o regulă care permite accesul, nu puteți folosi în acest fișier o altă regulă care să interzică accesul.

Un lucru important pe care trebuie să îl rețineți este acela că dacă în nici unul dintre fișierele de configurare nu este găsită o regulă corespunzătoare, accesul este permis în mod prestabilit. Mai târziu în acest capitol veți vedea cum puteți folosi cuvântul cheie ALL la sfârșitul fișierului hosts.deny pentru a interzice accesul gazdelor care nu sunt specificate în fișierul hosts.allow.

Configurarea fișierului *inetd.conf*

Primul fișier care trebuie editat este cel folosit de demonul inetd. Fiecare înregistrare este formată dintr-o singură linie și este folosită pentru un singur serviciu. Tabelul 13.1 descrie câmpurile care formează o înregistrare din acest fișier.

Tabelul 13.1 Câmpurile fișierului de configurare /etc/inetd

Numele câmpului	Descriere
Name (nume)	Numele serviciului, cum ar fi ftp sau telnet. Acest nume este folosit ca referință încrucișată în fișierul /etc/services, care conține numărul portului corespunzător fiecărui serviciu.
Data type (tip de date)	Poate avea valorile stream, datagram sau dgram, indicând un protocol orientat spre conexiune (flux) sau un protocol fără conexiune pentru serviciul respectiv.
Protocol	Protocolul de transport în rețea folosit de serviciu, cum ar fi tcp sau udp. Protocoalele sunt definite în fișierul /etc/protocols.
Wait-state (starea de așteptare)	wait sau nowait. Dacă are valoarea wait, programul demon inetd lansează un proces pentru o cerere, apoi așteaptă terminarea acestuia înainte de a deservi o altă cerere. Dacă are valoarea nowait, programul demon lansează un proces pentru o cerere, apoi continuă să asculte soclul pentru alte cereri, pe care le deservește fără să aștepte.
UID	Identificatorul de utilizator (UID, sau userID) sub care rulează procesul serviciului.
Server	Numele programului server pe care îl lansează demonul inetd pentru deservirea cererii.
Process arguments (argumentele procesului)	Argumentele în linia de comandă transmise programului serviciu. Primul argument este întotdeauna numele serviciului.

Unde este păstrat demonul tcpd?

Deși UNIX era prezentat odată ca un sistem de operare cu portabilitate universală, ar fi o greșală să-l considerăm astfel în prezent. Există multe implementări diferite ale sistemului de operare, iar locul de stocare a fișierelor nu este același în două versiuni ale unor producători diferiți. Nu copiați cuvânt cu cuvânt exemplele din acest capitol. Verificați documentația și fișierele de configurare ale sistemului dumneavoastră pentru a determina unde sunt păstrate fișierele executabile ale programelor demon și unde ar trebui să stocați demonul tcpd.

Reporniți demonul inetd după editarea fișierelor

După ce editați fișierul `inetd.conf`, trebuie să reporniți demonul `inetd`, astfel încât acesta să citească din nou fișierul și să ia în considerare modificările pe care le-ați făcut. Schimbările nu au efect decât după ce reporniți programul demon (sau după ce reîncărcați sistemul). Comanda folosită pentru repornirea demonului depinde de varianta de UNIX pe care o folosiți. Sub Solaris 7, de exemplu, puteți folosi următoarea comandă:

```
# pkill -HUP
inetd
```

Așa cum puteți vedea în tabelul 13.1, nici unul dintre câmpuri nu arată cine are dreptul să ruleze un anumit serviciu de rețea. Fișierul `inetd.conf` nu face decât să stabilească o corespondență între numele unui serviciu și programul executabil care va deservi cererea, împreună cu protocolul ce va fi folosit și identificatorul de utilizator sub care va rula programul.

TCP Wrappers poate fi folosit pentru a asigura controlul accesului. De exemplu, următoarea înregistrare din fișierul `inetd.conf` este folosită pentru lansarea serviciului FTP:

```
ftp stream tcp nowait root /usr/etc/in.ftpd in.ftpd
```

Pe baza acestei înregistrări, `inetd` va lansa executabilul definit de calea `/usr/etc/in.ftpd`. Pentru implicarea programului TCP Wrappers, această linie trebuie modificată astfel încât să fie lansat demonul `container`:

```
ftp stream tcp nowait root /usr/etc/tcpd in.ftpd
```

Trebuie să faceți această modificare în fiecare linie a fișierului `inetd.conf` care lansează un serviciu pe care vreți să îl folosiți prin TCP Wrappers. Înainte de a edita acest fișier, este o idee bună să faceți o copie de siguranță pe care să o aveți la dispoziție dacă faceți o greșală.

Fișierele `hosts.allow` și `hosts.deny`

După ce ați configurat demonul `tcpd` pentru gestionarea serviciilor de rețea, prin editarea fișierului `inetd.conf`, următorul lucru pe care trebuie să îl faceți este să editați celelalte două fișiere folosite pentru stocarea informațiilor despre cei care au voie (și cei care nu au voie) să folosească fiecare serviciu. Aceste fișiere sunt `hosts.allow` și `hosts.deny`. Atunci când le folosește, demonul `tcpd` citește mai întâi fișierul `allow`, apoi fișierul `deny`.

Sintaxa de bază pentru ambele fișiere este următoarea:

```
lista_demoni : lista_clienti : [: comanda_de_nucleu]
```

Pentru argumentul `lista_demoni` furnizați numele serviciului căruia i se aplică regula. Dacă specificați mai multe servicii pe aceeași linie, separați-le prin virgule. Pentru `lista_clienti`, folosiți un nume de gazdă, un nume de domeniu sau o adresă IP. La fel ca în cazul serviciilor, și în această parte a regulii puteți specifica mai multe gazde, separându-le prin virgule. Ultima parte a regulii este o comandă de nucleu, opțională. Această comandă opțională poate fi destul de utilă, așa cum veți vedea în exemplele următoare.

Un lucru foarte important pe care trebuie să îl rețineți este că `tcpd` folosește prima regulă care se potrivește și ignoră următoarele reguli. *Mai important este că, dacă nu găsește nici o regulă care să se potrivească în nici unul dintre cele două fișiere, accesul este permis în mod prestabilit!* Din acest motiv, ar trebui ca întotdeauna să interziceți tuturor explicit accesul, apoi să permiteți accesul selectiv numai celor cărora le este necesar!

Există câteva cuvinte cheie pe care le puteți folosi pentru acești parametri și care fac configurarea mai simplă:

- ALL – Acest cuvânt cheie poate fi folosit pentru specificarea tuturor serviciilor sau a tuturor gazdelor.
- LOCAL – Acest cuvânt cheie poate fi folosit pentru specificarea oricărui nume care nu conține caracterul punct.
- UNKNOWN – Acest cuvânt cheie poate fi folosit pentru specificarea oricărui utilizator al cărui nume nu este cunoscut sau a oricărei gazde cu nume sau adresă necunoscute.
- KNOWN – Acest cuvânt cheie poate fi folosit pentru specificarea oricărui utilizator al cărui nume este cunoscut sau a oricărei gazde cu nume și adresă cunoscute.
- PARANOID – Acest cuvânt cheie poate fi folosit pentru specificarea oricărei gazde al cărei nume nu corespunde adresei. Pentru folosirea acestui cuvânt cheie, trebuie să construiți demonul `tcpd` folosind opțiunea `-DPARANOID`.

În plus, există și un cuvânt cheie cu rol de operator, care poate fi folosit pentru a modifica o regulă: `EXCEPT`. Sintaxa acestui operator este următoarea:

```
lista1 EXCEPT lista2
```

În continuare sunt prezentate câteva exemple simple:

Iată cum arată fișierul `hosts.allow`:

```
ALL: localhost
in.telnetd : twoinc.com
inet.ftpd : zira.twoinc.com
```

Iată cum arată fișierul `hosts.deny`:

```
inet.telnetd : ritchie.twoinc.com
```

În fișierul `allow`, puteți vedea că toate gazdele din domeniul `twinc.com` au permisiunea să folosească demonul `Telnet`. O singură gazdă, `zira`, are permisiunea să folosească demonul `FTP`. Să presupunem că în domeniul `twinc.com` există o singură gazdă care nu asigură impunerea regulilor de securitate, `ritchie`, așa că vreți să interziceți accesul gazdei respective. Ultima linie din fișierul `hosts.deny` pare să facă acest lucru, dar în realitate nu funcționează. Demonul TCP Wrappers nu va ajunge niciodată la linia respectivă, deoarece asimilează adresa `ritchie.twoinc.com` cu domeniul `twinc.com`, specificat în fișierul `hosts.allow`. Din această cauză, demonul nu mai verifică restul fișierului și nici nu mai ajunge la fișierul `deny` pentru a citi înregistrarea despre care dumneavoastră credeți că va interzice accesul gazdei `ritchie`.

Pentru a impune o politică de securitate prin care este interzis tot ce nu este permis explicit, puteți insera în fișierul `hosts.deny` următoarea linie:

```
ALL:ALL
```

Apoi editați fișierul `hosts.allow` astfel încât să conțină numai gazdele cărora le veți permite accesul la serviciile de rețea. În această configurație, accesul este interzis tuturor gazdelor pe care demonul `tcpd` nu le găsește atunci când parcurge fișierul `hosts.allow`.

Și operatorul `EXCEPT` poate fi util. Iată un exemplu:

```
ALL : .twinc.com EXCEPT zira.twoinc.com
```

Dacă această linie este folosită în fișierul `hosts.allow`, tuturor gazdelor din domeniul `twoinc.com` le este permis accesul la toate serviciile, cu excepția gazdei numite `zira.twoinc.com`.

Opțional, pentru o regulă puteți folosi și o comandă de nucleu. Comanda pe care o inserați în aceste fișiere este lansată ca proces descendent, cu intrările, ieșirile și erorile direcționate către `/dev/null`. Atunci când folosiți comenzi de nucleu, ar trebui să specificați întotdeauna calea de acces completă a comenzii. Câteva dintre variabilele pe care le puteți folosi pentru substituie în comenzi sunt prezentate în tabelul 13.2.

Tabelul 13.2 Variabile pe care le puteți folosi cu comenzi de nucleu

Variabilă	Descriere
%a (sau %A)	Returnează adresa de gazdă a clientului (serverului).
%c	Returnează informații despre client. Poate fi <code>user@host</code> , <code>user@address</code> , doar un nume de gazdă sau doar o adresă. Valoarea returnată depinde de informațiile disponibile în implementarea pe care o aveți.
%d	Returnează numele procesului demon (obținut de <code>argv[0]</code>).
%h (sau %H)	Returnează numele de gazdă al clientului (serverului). Dacă acesta nu este disponibil, returnează adresa.
%n (sau %N)	Returnează numele de gazdă al clientului (serverului) sau una dintre valorile <code>unknown</code> ori <code>paranoid</code> .
%p	Returnează identificatorul procesului demon.
%s	Returnează informații despre server. Poate fi <code>daemon@host</code> , <code>daemon@address</code> sau doar numele demonului. Valoarea returnată depinde de informațiile disponibile în implementarea pe care o aveți.
%u	Returnează numele de utilizator al clientului sau valoarea <code>unknown</code> .
%%	Transformat într-un singur caracter %.

Iată un exemplu de folosire a unei comenzi de nucleu:

```
in.ftpd : .twoinc.com : (/usr/bin/safe_finger -l @%h |
/usr/ucb/mail -s %d-%h root) &
```

Dacă această regulă ar fi folosită în fișierul `hosts.deny`, utilizatorul `root` ar primi un mesaj e-mail atunci când regula ar interzice accesul pentru gazdele din domeniul `twoinc.com`. Remarcați că variabila `%h` este înlocuită cu numele de gazdă al clientului, iar variabila `-%d` este înlocuită cu numele serviciului.

Ce este `safe_finger`?

Pentru a evita problemele cauzate de ceea ce pot face hackerii de la distanță ca răspuns la o sondă `finger`, nu folosiți programul `finger` livrat împreună cu versiunea UNIX pe care o aveți. Așa cum se întâmplă cu toate programele UNIX scrise cu mai mulți ani în urmă, și programul `finger` are unele slăbiciuni ce pot fi exploatate de un

hacker cu cunoștințele necesare. Puteți să folosiți în schimb programul `safe_finger` din setul TCP Wrappers. Versiunile sigure (și există mai multe) sunt codate mai bine și pot fi configurate astfel încât să nu ofere prea multe informații celor care nu ar trebui să le vadă. La fel ca și alte componente ale pachetului, acesta este un program C care poate fi compilat pentru a fi rulat pe sistemul dumneavoastră.

Limitele produsului TCP Wrappers

Tabelul 13.2 prezintă variabilele de înlocuire ce pot fi folosite împreună cu comenzile de nucleu. Una dintre acestea, `%u`, depinde de posibilitatea de interogare a gazdei de proveniență a cererii, conform definiției din documentul RFC 931.

De asemenea, rețineți că TCP Wrappers nu ar trebui să fie singura linie de apărare a sistemului dumneavoastră. Adresele IP și numele de gazde pot fi falsificate. TCP Wrappers nu poate identifica întotdeauna aceste situații. Deoarece programul de încapsulare (wrapper) este folosit doar pentru lansarea inițială a demonului corespunzător care va deservi cererea, nu funcționează cu servicii precum NFS, care după lansare deservesc mai mulți clienți. Numai serviciile care sunt lansate pentru fiecare conexiune de către `inetd` pot folosi utilitățile TCP Wrappers. Procesele demon de fundal, lansate la încărcare prin intermediul fișierelor de pornire, nu funcționează în această manieră.

Ce este RFC 931?

RFC 931 definește protocolul Authentication Server Protocol. Acest protocol permite obținerea numelui de utilizator pe baza porturilor TCP folosite pentru o conexiune între două gazde. Serverul pentru acest protocol ascultă portul TCP 113. Atunci când este realizată o conexiune la acest port, serverul citește o linie de date care descrie conexiunea. Dacă pe server există conexiunea, către solicitant este returnat numele utilizatorului proprietar al conexiunii. Acest serviciu nu este implementat în toate versiunile UNIX sau în toate produsele TCP, așa că nu ar trebui să îl luați în calcul pentru orice situație. În plus, de la elaborarea documentului RFC 931 au apărut și alte documente, cum ar fi RFC 1413, schimbând numele serviciului în Identification Protocol (sau Ident Protocol).

În pachet sunt disponibile mai multe utilitare ce pot fi folosite pentru depanarea configurației. Programul `tcpdchk` poate examina regulile din fișierele `hosts.allow` și `hosts.deny`, raportând problemele pe care le descoperă. Programul `tcpdmatch` poate fi folosit pentru simularea modului în care va funcționa controlul accesului pentru regulile pe care le-ați creat. Sintaxa acestui program este următoarea:

```
tcpdmatch nume-proces nume-gazda
```

sau

```
tcpdmatch nume-proces adresa
```

Numele procesului este numele serviciului, așa cum apare acesta în fișierele de reguli. Numele de gazdă și adresa sunt numele sau adresa gazdei pe care vreți să o evaluați în condițiile regulilor stabilite.

Rezumat

Utilitarele TCP Wrappers pot fi folosite pentru a adăuga controlul accesului la serviciile TCP și UDP care rulează pe o gazdă din rețea sau pe o gazdă firewall. Deși nu este o soluție completă pentru toate cerințele de securitate, demonul de încapsulare (wrapper) poate fi foarte util, în special datorită posibilităților de înregistrare în jurnal pe care le oferă. Totuși, nu vă bazați numai pe aceste programe ca unică măsură de securitate. Nu uitați că un firewall este format din multe componente și cele pe care le alegeți depind de politica de securitate și de arhitectura rețelei și a firewall-ului.

Capitolul 14

Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)

- Construirea unui firewall folosind setul de instrumente FWTK
- Componentele setului FWTK
- Configurarea serviciilor intermediar
- Instalarea setului de instrumente pe o gazdă bastion

De ce setul de instrumente FWTK este gratuit?

TIS Internet Toolkit a fost dezvoltat în cadrul unui contract guvernamental care stipula ca întregul cod sursă rezultat să fie plasat în domeniul public. Codul este acum susținut de un număr mare de persoane și chiar îi este dedicat un sit Web: www.fwtk.org. De pe acest sit puteți selecta situl copie cel mai apropiat de dumneavoastră, de unde puteți descărca setul de instrumente și documentația.

Construirea unui firewall folosind setul de instrumente FWTK

TIS Internet Firewall Toolkit (FWTK) nu este o soluție comercială pentru firewall-uri. Așa cum sugerează și numele, este un set compus din mai multe instrumente diferite care, împreună cu o manieră corespunzătoare de administrare a sistemului, pot fi folosite pentru construirea unui firewall. FWTK este o soluție dedicată sistemelor UNIX și funcționează cu implementările TCP/IP care folosesc socluri de tip Berkeley. Totuși, chiar dacă aveți o rețea de calculatoare Windows NT sau Windows 98, cunoașterea setului de instrumente FWTK vă poate fi de folos. S-ar putea să descoperiți că flexibilitatea oferită de posibilitatea de construire a unui firewall pornind de la zero, astfel încât să corespundă exact politicilor de securitate ale rețelei dumneavoastră, poate justifica prețul plătit pentru instalarea unei mașini UNIX la frontiera rețelei.

O scurtă istorie a setului de instrumente FWTK

FWTK are o istorie lungă. A fost dezvoltat inițial de o companie numită Trusted Information Systems, Inc., pentru agenția DARPA (Defense Advanced Research Projects Agency). Atunci când a fost creat FWTK, singura protecție de tip firewall disponibilă era

filtrul elementar de pachete. Deși un filtru de pachete își are locul în strategia de implementare a unui firewall, era nevoie de ceva mai mult pentru impunerea politicii de securitate a firewall-ului, iar FWTK a fost dezvoltat tocmai în acest scop.

FWTK nu este un filtru de pachete, ci o colecție de diferite programe pe care le puteți folosi ca să creați servere intermediar pentru cele mai populare servicii TCP/IP. Rețineți că un firewall bun este construit, de obicei, folosind atât filtrarea pachetelor, cât și servere intermediar. Deși FWTK nu asigură filtrarea pachetelor, poate funcționa destul de bine pe gazdele bastion protejate de un ruter cu filtrarea pachetelor.

Obținerea setului de instrumente FWTK

FWTK este disponibil gratuit în Web. Folosiți mai întâi browserul Web ca să ajungeți la situl www.fwtk.org. De aici, alegeți cel mai apropiat sit copie. Executați clic pe legătura care indică descărcarea codului și citiți condițiile de licențiere a produsului software. Dacă sunteți de acord cu acestea, trebuie să trimiteți un mesaj prin care comunicați faptul că acceptați condițiile pentru a vi se permite să descărcați codul. Trimiteți mesajul e-mail la adresa fwtk-request@tislabs.com. În corpul mesajului scrieți cuvântul „accepted” (fără ghilimele). Pentru a primi un răspuns de la TIS, acest cuvânt trebuie să apară în corpul mesajului, nu pe linia de subiect.

În scurt timp ar trebui să primiți din partea TIS un răspuns automatizat. Acest mesaj va conține numele unui director temporar de pe situl ftp.tislabs.com, pe care îl puteți folosi pentru descărcarea componentelor software și a documentației. Acest director temporar există numai 12 ore, așa că ar fi bine să începeți descărcarea cât mai repede după primirea mesajului. Dacă nu reușiți să descărcați fișierele până la expirarea timpului, trimiteți o altă cerere prin e-mail și veți primi numele unui alt director temporar.

Căutarea inversă a numelor

Calculatorul gazdă pe care îl folosiți pentru descărcarea setului de instrumente trebuie să permită căutarea inversă a numelor. Deși funcția normală a unui server DNS este de a transforma un nume într-o adresă IP, căutarea inversă a numelor este folosită pentru a transforma o adresă IP într-un nume. Acest lucru este făcut din motive de securitate, pentru a verifica dacă într-adevăr sunteți cine susțineți că sunteți.

După ce descărcați componentele software, nu uitați să citiți fișierele readme ca să aflați ultimele informații despre compilarea și utilizarea componentelor din setul de instrumente, care sunt furnizate sub formă de cod sursă. Ca urmare, trebuie să le compilați înainte de a le putea folosi pe sistemul dumneavoastră. Acestea nu sunt furnizate ca o aplicație deja pregătită, cu un program de instalare care să automatizeze procesul. Pentru o utilizare corespunzătoare a setului de instrumente, trebuie să înțelegeți bine protocolul TCP/IP și sistemul de operare UNIX. Acesta nu este un produs pentru începători. Dacă nu înțelegeți cum funcționează componentele individuale și cum este configurat sistemul de operare, este aproape imposibil să folosiți setul de instrumente cu siguranța că ați făcut tot ce se putea pentru a asigura securitatea rețelei. Deoarece setul de instrumente este scris în limbajul de programare C, ar trebui să cunoașteți bine și acest limbaj.

Care sunt diferențele între firewall-ul Gauntlet și FWTK?

După ce TIS a dezvoltat setul de instrumente FWTK, compania a mers mai departe, creând firewall-ul Gauntlet. În 1998, TIS a fuzionat cu o altă companie, Network Associates, iar aceasta încă vinde firewall-ul Gauntlet. La prima vedere, există multe asemănări între cele două produse, și mulți cred că FWTK este doar o versiune redusă a firewall-ului Gauntlet. Totuși, începând cu versiunea 1.0, cele două produse nu mai folosesc același cod sursă. Sursele pentru Gauntlet sunt disponibile – contra cost – așa că puteți să le comparați dacă doriți.

FWTK nu asigură întregul set de servicii oferit de Gauntlet. Iată ce oferă setul de instrumente FWTK:

- Cod sursă
- Servere intermediar pentru FTP, TELNET, Rlogin, HTTP, Gopher, SMTP, NNTP
- Poartă X11 (X11 Gateway)
- Server de autentificare (Authentication Server)
- Diferite instrumente pentru testarea firewall-ului

La acestea, Gauntlet adaugă alte servere intermediar, compatibilitatea cu SSL, SHTTP și POP3, un server DNS și multe alte caracteristici. Desigur, deoarece Gauntlet este un produs comercial, TIS oferă și instruire și asistență tehnică. FWTK este un produs întreținut de utilizatorul final și nu puteți obține alt ajutor în afară de ceea ce oferă situl Web dedicat și cei care participă la grupurile de discuții sau listele poștale. Totuși, dacă aveți cunoștințele necesare despre administrarea unui sistem UNIX și despre TCP/IP, setul de instrumente ar putea fi tocmai ceea ce căutați.

Componentele setului FWTK

Așadar, ce obțineți atunci când descărcați setul de instrumente? Documentația furnizată de TIS precizează că setul de instrumente este format din trei componente:

- Filozofia de proiectare
- Practici de configurare și strategii de verificare
- Instrumente software

Deși ați putea considera că ultimul articol din această listă este cea mai importantă parte a setului, nu este întotdeauna așa. Pentru a folosi corespunzător instrumentele oferite de set, trebuie să înțelegeți bine ce faceți cu acestea. Componenta „filozofie de proiectare” din set stabilește câteva principii importante. De exemplu, atunci când implementați un firewall, ar trebui să îl configurați astfel încât nici o gazdă dintr-o rețea careia nu i s-a acordat încredere (Internet, de exemplu) să nu poată realiza o conexiune directă cu un serviciu de rețea care rulează cu privilegii în rețeaua dumneavoastră. Toate serviciile de rețea pe care le oferiți ar trebui să fie realizate prin aplicații codate simplu, nu prin aplicații mari și complexe care sunt dificil de înțeles și, ca urmare, expuse la erori. După ce configurați firewall-ul, ar trebui să aveți posibilitatea să îl testați complet, astfel încât să vă convingeți că face ceea ce vă așteptați.

Practicile de configurare, a doua componentă, implică faptul că ar trebui să configurați firewall-ul ținând seama de arhitectura rețelei și de politicile de securitate. În capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, am prezentat unele strategii de creare a firewall-urilor, cum ar fi gazdele cu două plăci de rețea, gazdele ecranate și subrețelele ecranate. De asemenea, am discutat despre tehnicile de creare a unei zone demilitarizate, astfel încât serviciile de rețea să poată fi oferite de gazde bastion aflate în afara rețelei locale, dar nu direct în Internet. Trebuie să știți ce strategie funcționează cel mai bine în mediul dumneavoastră înainte de a începe să folosiți instrumentele oferite de FWTK.

Ce este o „cutie de cristal”?

Termenul „cutie neagră” este folosit, de obicei, pentru a descrie un sistem în care sunt cunoscute intrările și ieșirile, dar nu și funcționarea internă. Nu aceasta este filozofia aplicată în cazul setului de instrumente. Acesta este dezvoltat ca o „cutie de cristal”. Codul sursă nu este păstrat secret prin compilarea componentelor, ci este pus la dispoziția oricui vrea să îl studieze.

Ideea aflată la baza acestei maniere de lucru este aceea că, făcând cunoscut codul sursă al componentelor setului de instrumente – atât utilizatorilor, cât și hackerilor – corectarea erorilor și distribuirea corecturilor prin Internet se simplifică. În loc să aștepte ca un furnizor să răspundă la o nouă amenințare de securitate, utilizatorii care asigură suportul pentru setul de instrumente prin Internet pot să elaboreze rapid un program de corectare sau o cale ocolitoare și să o pună la dispoziția tuturor.

Un exemplu din setul de instrumente pentru practicile de configurare este serviciul FTP. Pentru a îmbunătăți securitatea operațiilor FTP anonime, setul de instrumente descrie utilizarea unei alte componente, `netacl`, pentru a oferi o versiune mai sigură a acestui serviciu.

Instrumentele software incluse în set sunt următoarele:

- `netacl` pentru asigurarea serviciilor Telnet, Finger și liste pentru controlul accesului la rețea.
- `smap` și `smapd` pentru asigurarea unui serviciu SMTP sigur.
- `ftp-gw` pentru asigurarea unui server intermediar pentru FTP.
- `tn-gw` pentru asigurarea unui server intermediar pentru Telnet.
- `rlogin-gw` pentru asigurarea unui server intermediar pentru Rlogin.
- `plug-gw` pentru asigurarea unui server intermediar generic.
- `authd` pentru asigurarea unui serviciu de autentificare care să îmbunătățească practicile de „autentificare puternică”.
- `telnetd` un server Telnet care poate fi folosit pentru gestionarea firewall-ului.
- `login-sw` un program de conectare îmbunătățit care asigură suportul pentru conexiuni sigure, folosind dispozitive de autentificare de tip token, cum ar fi cartelele inteligente.
- `syslogd` un înlocuitor pentru demonul de conectare UNIX tradițional.

Restul acestui capitol va prezenta mai detaliat câteva dintre componentele menționate mai sus.

netacl

Programul `netacl` din setul de instrumente funcționează ca un program pentru controlul accesului. Acest program este furnizat în setul de instrumente astfel încât să puteți permite utilizarea pe un firewall a unor servicii de rețea într-o manieră mai sigură. De exemplu, puteți folosi programul `netacl` pentru a rula serverul Telnet pe un firewall, dar stabilind reguli care permit numai anumitor gazde – cum ar fi stația de lucru a administratorului – să utilizeze acest server. Datorită modului în care poate fi configurat programul `netacl`, puteți chiar să specificați un demon Telnet diferit pentru fiecare utilizator. Deși am ales ca exemplu serviciul Telnet, puteți folosi programul `netacl` pentru a rula diverse alte servicii de rețea pe gazda firewall. Deoarece `netacl` poate fi folosit pentru a oferi administratorului acces prin rețea la firewall, vom discuta despre acesta înainte de a prezenta aplicațiile intermediar din setul de instrumente.

Ca și alte servere intermediar din setul de instrumente, programul `netacl` folosește un fișier numit `/usr/local/etc/netperm-table` pentru a decide dacă un serviciu este permis sau nu, pe baza numelui de gazdă sau a adresei IP a calculatorului care a generat cererea. Pentru a înțelege cum funcționează programul `netacl`, să vedem mai întâi cum sunt lansate în mod obișnuit serviciile de rețea.

În sistemele UNIX, responsabilitatea lansării serviciilor de rețea revine demonului `inetd`, iar serviciile sunt configurate în fișierul `/etc/inetd.conf`. Acest fișier conține o listă de servicii și de informații de care demonul `inetd` are nevoie pentru asigurarea serviciului. Tabelul 14.1 descrie câmpurile fiecărei linii din fișierul de configurare.

Tabelul 13.1 Câmpurile fișierului de configurare `/etc/inetd`

Numele câmpului	Descriere
Name (nume)	Numele serviciului, cum ar fi „FTP” sau „Telnet”. Acest nume este folosit ca referință încrucișată în fișierul <code>/etc/services</code> , care conține numărul portului corespunzător fiecărui serviciu.
Data type (tip de date)	Poate avea valorile <code>stream</code> , <code>datagram</code> sau <code>dgram</code> , indicând un protocol orientat spre conexiune (flux) sau un protocol fără conexiune pentru serviciul respectiv.
Protocol	Protocolul de transport în rețea folosit de serviciu, cum ar fi TCP sau UDP. Protocoalele sunt definite în fișierul <code>/etc/protocols</code> .
Wait-state (starea de așteptare)	Poate avea valorile „wait” sau „nowait”. Dacă are valoarea <code>wait</code> , programul demon <code>inetd</code> lansează un proces pentru o cerere, apoi așteaptă terminarea acestuia înainte de a deservi o altă cerere. Dacă are valoarea <code>nowait</code> , programul demon lansează un proces pentru o cerere, apoi continuă să asculte soclul pentru alte cereri, pe care le deservește fără să aștepte.
UID	Identificatorul de utilizator (UID, sau userID) sub care rulează procesul serviciului.

continuare

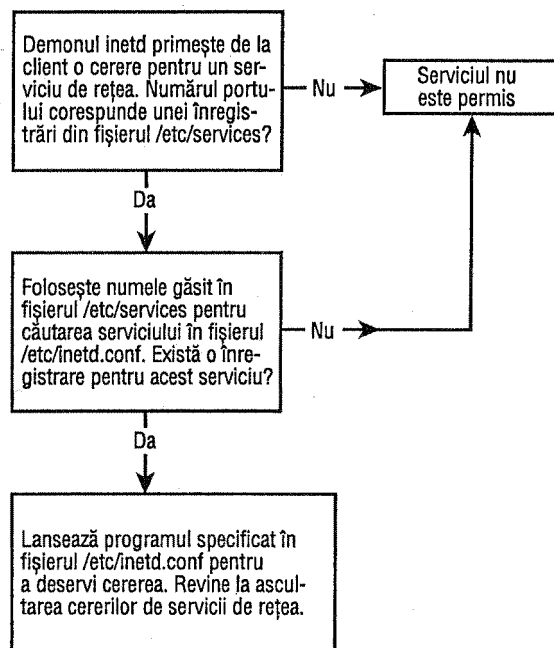
Tabelul 13.1 Continuare

Numele câmpului	Descriere
Server	Numele programului server pe care îl lansează demonul inetd pentru deservirea cererii.
Process arguments (argumentele procesului)	Argumentele în linia de comandă transmise programului serviciu. Primul argument este întotdeauna numele serviciului.

Așa cum puteți vedea în figura 14.1, demonul inetd rulează ca proces de fundal și ascultă cererile din rețea. Pentru generarea unei cereri, către server este trimis un pachet care conține atât adresa IP a expeditorului, cât și un număr de *port*. Numărul portului este folosit de demon pentru a determina ce serviciu este solicitat. Fișierul `/etc/services` este folosit pentru căutarea numărului de port și, după ce numele serviciului este cunoscut, programul demon poate folosi informațiile din fișierul `/etc/inetd.conf` pentru a determina dacă serviciul este permis pentru serverul respectiv și, în caz afirmativ, ce program să ruleze pentru deservirea cererii.

FIGURA 14.1

Demonul inetd ascultă cererile de servicii de rețea și lansează programul folosit pentru deservirea cererii.



Vezi și

- Pentru mai multe informații despre modul în care sunt folosite porturile de protocoalele TCP și UDP, vezi pagina 46.
- Pentru o listă a porturilor TCP și UDP recunoscute, vezi pagina 318.

Reporniți demonul inetd după ce editați fișierul `/etc/inetd.conf`!

Deoarece demonul inetd citește fișierul de configurare numai la pornire, trebuie să reporniți demonul (sau să reîncărcați sistemul) după ce editați fișierul `/etc/inetd.conf`.

Listingul 14.1 prezintă ca exemplu o porțiune din fișierul `/etc/inetd.conf`.

Listingul 14.1 Exemplu de fișier `/etc/inetd.conf`

```

#
# /etc/inetd.conf
#
ftp          stream    tcp      nowait    root     /usr/etc/in.ftpd
in.ftpd
telnet       stream    tcp      nowait    root     /usr/etc/in.telnetd
in.telnetd
shell        stream    tcp      nowait    root     /usr/etc/in.rshd
in.telnetd
login        stream    tcp      nowait    root     /usr/etc/in.rlogind
in.rlogind
tftp         dgram     udp      wait      root     /usr/etc/in.tftpd
in.tftpd
finger       stream    tcp      nowait    nobody   /usr/etc/in.fingerd
in.fingerd
...
#
# end

```

În acest listing puteți vedea că serviciile obișnuite de rețea, cum ar fi FTP și telnet, sunt asigurate de firewall prin lansarea programelor asociate. Totuși, din acest fișier lipsește o funcționalitate importantă. Nu există nici o metodă de control al accesului. Demonul inetd nu face decât ce îi cere o înregistrare din acest fișier. Nu are nici un mecanism prin care să decidă dacă o anumită gazdă care a lansat cererea are dreptul să folosească serviciul. Această parte este lăsată în seama procedurilor obișnuite de autentificare ale sistemului, care implică un nume de utilizator și o parolă, stocate în fișierul `/etc/passwd`. Deoarece această metodă de autentificare nu este foarte puternică – de exemplu, serviciul telnet transmite numele de utilizator și parolele sub formă de text clar, care poate fi interceptat – de fapt nu este o metodă sigură pentru oferirea serviciilor pe o gazdă firewall.

netac1 nu acceptă protocolul UDP

Aplicația netac1 poate fi folosită numai pentru serviciile bazate pe protocolul TCP. Nu poate fi folosită pentru serviciile bazate pe UDP, deoarece este aproape imposibil să verificați fără dubii originea unui pachet UDP. Dacă vreți să folosiți un serviciu bazat pe UDP, utilizați o aplicație de încapsulare TCP (TCP wrapper).

Pentru a compensa această lipsă de control al accesului, este folosit programul netac1. Pentru a utiliza programul netac1 cu un serviciu de rețea, trebuie să editați acest fișier. În loc să apelați programul `in.ftpd` pentru deservirea unei cereri FTP, apelați programul `netac1` și îl lăsați apoi să se ocupe de lansarea demonului server pentru gazda care a făcut

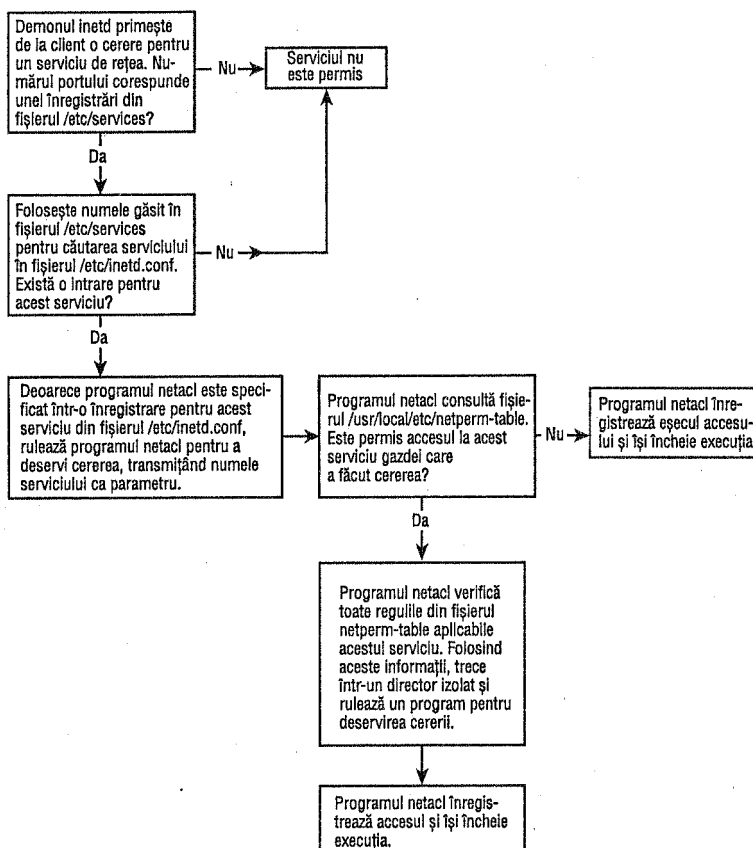
cererea. Un exemplu de înregistrare din fișierul `/etc/inetd.conf` pentru serviciul FTP ar arăta astfel:

```
ftp      stream    tcp      nowait   root    /usr/local/etc/netacl
➔in.ftpd
```

După cum puteți vedea în acest exemplu, câmpul `Server` din fișierul `/etc/inetd.conf` apelează acum programul `netacl` în locul programului `server` FTP. Argumentul transmis programului `netacl` este numele serviciului. Totuși, înainte de a putea să lanseze programul `server`, `netacl` trebuie să mai parcurgă o etapă. Trebuie să caute în fișierul `/usr/local/etc/netperm-table` o înregistrare corespunzătoare serviciului FTP, pentru a decide dacă rularea acestuia este permisă pentru gazda care a făcut cererea și, în caz afirmativ, să stabilească programul ce trebuie rulat pentru asigurarea serviciului și identificatorul de utilizator (UID sau userID) sub care va rula acesta. În figura 14.2 puteți vedea că acest proces nu face decât să adauge câteva etape la procesul normal de lansare a unui serviciu de rețea.

FIGURA 14.2

Programul `netacl` este apelat de `inetd` pentru a răspunde la o cerere de serviciu.



Fișierul de configurare: `/usr/local/etc/netperm-table`

Când este lansat de `inetd`, `netacl` nu începe imediat rularea serviciului solicitat, care este transmis ca argument în linia de comandă. Mai întâi preia acest unic argument și îl folosește pentru a căuta informații despre serviciu într-o bază de date cu reguli, definită în fișierul `/usr/local/etc/netperm-table`. Vă puteți gândi la acest fișier ca la o sursă centrală de informații de configurare pentru toate aplicațiile intermediar care formează setul de instrumente. Imediat ce programul `netacl` (sau o altă aplicație intermediar din set) este executat, citește informațiile de configurare din acest fișier și le stochează în memorie. Ca urmare, după ce aplicația folosește comanda `chroot` pentru a trece într-un alt director, informațiile rămân disponibile și nu este nevoie ca fișierul să rămână accesibil în timpul rulării serviciului. Prin folosirea acestei metode, aveți siguranța că o hibă din programul serviciu nu poate fi folosită pentru accesul neautorizat la fișierul `netperm-table`.

Fiecare linie din fișierul `netperm-table` este numită *regulă*. Fiecare regulă poate fi aplicată uneia sau mai multor aplicații din setul de instrumente și este formată din două componente importante:

- **Cuvânt cheie** Acesta este numele aplicației (aplicațiilor) asupra căreia (căror) se aplică regula. Acest nume este textul care denumește serviciul și îl puteți obține din fișierul `/etc/services`. Atunci când serviciul este folosit împreună cu aplicația `netacl`, numele este compus din textul „`netacl-`”, plus numele serviciului. Numele este separat de restul regulii printr-un caracter două puncte (:). Separați numele multiple de pe aceeași linie prin virgule. Puteți folosi caractere de înlocuire pentru a specifica mai multe aplicații.
- **Lista de valori pentru atribut** Acesta este de fapt textul care definește regula pentru aplicația asociată. Partea de atribut este un parametru de configurare pentru aplicație și este urmată de una sau mai multe valori pentru parametrul respectiv.

Cât de lungă poate fi o regulă?

Lungimea maximă a unei reguli depinde de sistemul pe care îl folosiți, dar ideea generală este că regula trebuie să încapă pe o linie. Nu există nici un „caracter de continuare a liniei” pe care să îl folosiți pentru a permite unei reguli să se întindă pe mai multe linii. Pentru cele mai multe sisteme, lungimea maximă pe care o poate avea o linie este de 1.024 de octeți.

Puteți insera în fișier comentarii, pentru a face mai ușor de înțeles aceste înregistrări pe o singură linie. Pentru a indica un comentariu, plasați un caracter „#” la începutul liniei. De asemenea, rețineți că atunci când o aplicație citește acest fișier pentru a găsi o regulă care i se aplică, o face de sus în jos și ține seama de ordinea în care apar regulile.

Ca urmare, dacă creați două reguli pentru aceeași aplicație, numai prima va fi folosită. Atunci când modificați acest fișier, verificați toate înregistrările, astfel încât să nu creați din greșeală reguli duplicate. O regulă duplicată nu înseamnă două reguli aplicate aceleiași aplicații intermediar. De fapt, deseori este necesar să creați mai multe reguli folosite de aceeași aplicație intermediar. O regulă ar putea fi folosită pentru definirea gazdelor care folosesc aplicația intermediar, în timp ce o altă regulă ar putea fi folosită pentru definirea directorului în care trece aplicația intermediar după ce este apelată. Un exemplu de regulă duplicată ar fi crearea a două reguli care specifică directorul. În acest caz, numai prima definire a directorului va fi folosită.

Un alt concept pe care trebuie să îl rețineți este că la verificarea valorii atributului pentru un nume de gazdă sau o adresă IP, comparația se face ținându-se seama dacă regula conține numai caractere numerice (și caracterul punct) sau conține caractere alfanumerice, indicând un nume de gazdă. Iată două exemple de reguli:

```
netacl-in.ftpd: permit-hosts yoko.twoinc.com -exec /usr/etc/in.ftpd
```

și

```
netacl-in.ftpd: permit-hosts 140.176.177.69 -exec /usr/etc/in.ftpd
```

În primul caz, regula conține un nume de gazdă, așa că aplicația va obține numele gazdei care a făcut cererea și îl va compara cu numele specificat în regulă. În al doilea caz, regula conține numai caractere numerice și puncte, așa că pentru comparație este folosită adresa IP a gazdei. În general, ar trebui să folosiți cea de-a doua formă. De ce? Deoarece este foarte ușor să folosiți înșelarea DNS pentru ca numele de gazdă să pară a fi altul decât cel real.

Puteți folosi caractere de înlocuire pentru ca o regulă să fie aplicată mai multor gazde. De exemplu, în loc să creați un număr mare de reguli, pentru fiecare gazdă din rețea căreia vreți să îi permiteți (sau să îi interziceți) accesul, puteți folosi un format asemănător cu cel din exemplul următor:

```
netacl-in.ftpd: permit-hosts 140.176.177.* -exec /usr/etc/in.ftpd
```

În acest caz, regula va permite tuturor gazdelor din rețeaua 140.176.177.0 să folosească aplicația lansată de netacl.

Ce sunt gazdele necunoscute (unknown)?

În urma încercării de transformare a unei adrese IP în numele de gazdă asociat, este returnat textul „unknown” dacă operația de căutare inversă eșuează. Puteți folosi textul „unknown” într-o regulă, în locul adresei IP sau al numelui de gazdă. Un exemplu ar fi folosirea modificatorului „deny-”, împreună cu textul „unknown” pentru a interzice acestor gazde folosirea aplicației intermediar.

În exemplele anterioare, a fost folosit modificatorul „permit-” împreună cu atributul „hosts”. Modificatoarele „permit-” și „deny-” pot fi folosite împreună cu unele dintre atributele acceptate în reguli. Atributele care pot fi folosite în fișier depind de aplicația căreia i se aplică regula. Paginile de manual („man pages”) furnizate împreună cu setul de instrumente specifică atributele ce pot fi folosite pentru fiecare aplicație. În exemplele pe care tocmai le-ați văzut, a fost folosit atributul „hosts” (permit-hosts). Aplicația intermediar ftp-gw permite și folosirea atributului denial-msg *fișier*, care specifică fișierul ce conține textul afișat pe ecranul unui utilizator căruia regula nu îi permite accesul la aplicație.

În plus, unele aplicații vă permit să specificați opțiuni, folosind în regulă caracterul „-”. În cazul aplicației intermediar ftp-gw (furnizată în setul de instrumente), următorul exemplu prezintă folosirea opțiunii -log:

```
ftp-gw: hosts 140.176.177.* -log {retr stor}
```

Remarcați că în acest exemplu numele aplicației nu este prefixat de textul „netacl-”, deoarece aplicația intermediar ftp-gw este cea căreia îi este aplicată regula. Regula nu este aplicată în cazul folosirii programului netacl pentru executarea demonului FTP obișnuit din sistemul de operare. De asemenea, această regulă nu permite și nu interzice unei gazde folosirea aplicației, ci doar definește opțiunile de înregistrare în jurnal pentru toate gazdele

din rețeaua 140.176.177.0. Parametrii încadrați de acolade ({retr stor}) specifică înregistrarea în jurnale a acestor acțiuni ale aplicației intermediar FTP (atunci când sunt executate de gazdele identificate de regulă). Ca urmare, deși scopul cel mai evident al regulilor din fișierul netperm-table este controlul accesului, acestea pot fi folosite și pentru configurarea unor opțiuni ale serviciilor rulate.

Tabelul 14.2 prezintă cuvintele cheie ce pot fi folosite în fișierul netperm-table pentru configurarea programului netacl.

Tabelul 14.2 Cuvintele cheie pentru atributele de configurare folosite împreună cu programul netacl

Cuvânt cheie	Descriere
hosts gazde	Specifică o regulă de stabilire a permisiunilor pentru gazde. Împreună cu acest cuvânt cheie puteți folosi modificatoarele permit- și deny-.
-exec program [argumente]	Specifică programul executabil rulat pentru serviciul căruia i se aplică această regulă. Trebuie să fie ultima opțiune a regulii. Atunci când folosiți programul netacl, toate regulile trebuie să conțină opțiunea -exec.
-user identificator de utilizator	Specifică utilizatorul (ca identificator numeric sau ca text reprezentând numele de utilizator). Acest utilizator trebuie să existe în fișierul /etc/passwd.
-chroot director	Directorul în care va trece netacl <i>înainte</i> de a apela programul executabil pentru serviciu. Deoarece comanda chroot este executată înainte de lansarea serviciului, programul executabil (specificat de opțiunea -exec) trebuie să aibă o cale de acces relativă la acest director.
timeout secunde	Numărul de secunde în care demonul poate rămâne în așteptare înainte de a fi deconectat. Duratele de așteptare FTP au, de obicei, valori între 300 de secunde (5 minute) și 3600 de secunde (1 oră). Este de dorit să folosiți valori mai mici atunci când serviciul FTP este folosit printr-un firewall, astfel încât conexiunile să nu rămână deschise o perioadă lungă de timp.

Cuvintele cheie ce pot fi folosite cu fiecare aplicație intermediar furnizată în setul de instrumente sunt prezentate în secțiunile care urmează, dedicate fiecărei aplicații.

Configurarea serviciilor intermediar

Setul de instrumente oferă aplicații intermediar „de trecere” pentru serviciile de rețea TCP/IP folosite în mod obișnuit. Fiecare dintre aceste aplicații ar trebui să fie configurată prin plasarea regulilor în fișierul netperm-table, la fel ca pentru programul netacl. Rețineți că prima parte a regulii, respectiv porțiunea de nume, *nu* trebuie să fie prefixată de textul netacl-.

FTP: *ftp-gw*

Aplicația *ftp-gw* vă permite să asigurați o aplicație intermediar pentru serviciul de rețea FTP. Prin configurarea aplicației intermediar (cu ajutorul regulilor din fișierul *netperm-table*), puteți asigura controlul accesului (ce gazde pot folosi serviciul), opțiuni de înregistrare în jurnal și destinații selectate pe blocuri. Aplicația intermediar *ftp-gw* trece mai întâi într-un director izolat și gol, astfel încât să nu creeze un risc de securitate pentru firewall. De asemenea, aplicația intermediar nu execută operații de intrare/ieșire locale (exceptând citirea informațiilor din fișierul de configurare *netperm-table*).

Rularea programului *ftp-gw* și a altor aplicații intermediar ca procese demon

Programul *ftp-gw* și alte aplicații intermediar din setul de instrumente pot fi rulate ca procese demon, caz în care ar trebui să plasați o înregistrare în fișierul */etc/rc.local*. De exemplu, atunci când *ftp-gw* este lansat în acest mod, va asculta portul FTP standard – portul 21. Pentru a schimba acest port cu unul nestandard, folosiți opțiunea în linie de comandă *-daemon port*.

Tabelul 14.3 prezintă cuvintele cheie ce pot fi folosite în fișierul *netperm-table* pentru configurarea programului intermediar *ftp-gw*.

Tabelul 14.3 Cuvintele cheie pentru atributele de configurare folosite împreună cu programul intermediar *ftp-gw*

Cuvânt cheie	Descriere
<i>authserver gazda port</i>	Specifică numele gazdei care rulează un server de autentificare și portul folosit pentru acest serviciu.
<i>denial-msg fisier</i>	Indică un fișier ce conține textul afișat utilizatorilor cărora nu li se permite accesul la aplicația intermediar <i>ftp-gw</i> . Dacă nu folosiți această opțiune, este generat un mesaj prestabilit.
<i>dendest-msg fisier</i>	Indică un fișier ce conține textul afișat utilizatorilor care încearcă să obțină acces la o destinație pentru care nu au permisiunea necesară. Dacă nu folosiți această opțiune, este generat un mesaj prestabilit.
<i>hosts gazde</i>	Folosit pentru specificarea uneia sau mai multor gazde, precum și a opțiunilor pentru acestea.
<i>directory director</i>	Folosit pentru specificarea directorului pe care îl va folosi aplicația intermediar înainte de a începe furnizarea serviciului pentru utilizator.
<i>groupid grup</i>	Folosit pentru a specifica grupul folosit de aplicația intermediar pentru rulare.
<i>help-msg fisier</i>	Indică un fișier care conține textul afișat utilizatorului atunci când acesta folosește comanda <i>help</i> . Dacă nu folosiți această opțiune, aplicația intermediar afișează o listă de comenzi.

Cuvânt cheie	Descriere
<i>timeout secunde</i>	Numărul de secunde în care aplicația intermediar poate rămâne în așteptare înainte de a fi deconectată.
<i>userid utilizator</i>	Folosit pentru a specifica numele sau identificatorul de utilizator (UID) sub care va rula aplicația intermediar.
<i>welcome-msg fisier</i>	Indică un fișier care conține un text de întâmpinare prezentat utilizatorului. Dacă nu folosiți această opțiune, este generat un mesaj prestabilit.

Așa cum puteți vedea, aplicația intermediar *ftp-gw* are mai multe atribute decât programul *netac1*. Procesul de configurare se complică și mai mult, deoarece atributul *hosts* permite folosirea mai multor opțiuni. Aceste opțiuni sunt prezentate în tabelul 14.4. Atunci când folosiți aceste opțiuni pentru atributul *hosts*, nu uitați să le prefixați cu un caracter „-”, așa ca în tabel.

Tabelul 14.4 Opțiuni pentru atributul *hosts*

Opțiune	Descriere
<i>-noinput</i>	Folosită pentru a specifica faptul că aplicația intermediar nu acceptă intrări printr-un port. Dacă se face o încercare, conexiunea este închisă.
<i>-nooutput</i>	Folosită pentru a specifica faptul că aplicația intermediar nu transmite rezultate (ieșiri) printr-un port. Dacă se face o încercare, conexiunea este închisă.
<i>-log operatie</i> sau <i>-log {operatia1 operatia2 ...}</i>	Această opțiune controlează înregistrările în jurnal pentru gazdele asociate. Puteți specifica una sau mai multe operații ale demonului FTP cu această opțiune.
<i>-authall</i>	Dacă este folosită această opțiune, aplicația intermediar nu permite executarea nici unei operații FTP (exceptând <i>quit</i>) până la autentificarea utilizatorului pe server.
<i>-auth operatie</i> sau <i>-auth {operatia1 operatia2 ...}</i>	Operațiile FTP pe care le specificați prin această opțiune <i>nu vor fi permise</i> până la autentificarea utilizatorului pe server.
<i>-dest destinatie</i> sau <i>-dest {destinatia1 destinatia2 ...}</i>	Această opțiune specifică destinațiile valide către care utilizatorul poate executa o operație FTP. Folosiți caracterul „!” pentru interzicerea unei destinații. Destinațiile pot fi specificate ca adrese IP sau ca nume de domenii și pot conține caractere de înlocuire.
<i>-deny operatie</i> sau <i>-auth {operatia1 operatia2 ...}</i>	Folosiți această opțiune pentru a specifica una sau mai multe operații FTP care nu sunt permise. Dacă nu folosiți această opțiune, toate comenzile FTP sunt accesibile utilizatorilor.

La prima vedere, toate aceste elemente pe care le puteți include în fișierul `netperm-table` pentru configurarea aplicației intermediar `ftp-gw` pot părea copleșitoare. Totuși, în cele mai multe situații veți folosi un număr mic de opțiuni. Pentru câteva dintre opțiunile din tabelul 14.4 este necesar un studiu mai aprofundat. Mai precis, pentru a obține o listă a operațiilor FTP pe care le puteți specifica folosind opțiunile `-log`, `-auth` și `-deny`, consultați paginile de manual din sistemul de operare UNIX. Deși aceasta este o listă lungă, operațiile cel mai frecvent folosite, pe care probabil le veți recunoaște, sunt `retr` și `stor`, care obțin, respectiv stochează fișiere.

În continuare, să vedem câteva exemple de reguli de configurare ce pot fi folosite în fișierul `netperm-table`:

```
ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt
ftp-gw: denial-msg /usr/local/etc/ftp-denial.txt
ftp-gw: help-msg /usr/local/etc/help-ftp.txt
ftp-gw: timeout 2400
ftp-gw: permit-hosts 140.176.177.*
ftp-gw: permit-hosts *--authall -log {retr stor}
```

În aceste exemple ați văzut cum puteți specifica fișierele de text pentru mesajele de întâmpinare, de interdicere sau de asistență (`help`). Durata de așteptare pentru o conexiune este stabilită la 2400 de secunde, după o care conexiune aflată în așteptare este închisă. Gazdelor din rețeaua 140.176.177.0 le este permis accesul la aplicația intermediar, în timp ce toate celelalte gazde (*) trebuie să fie autentificate pentru toate operațiile, iar operațiile de obținere și stocare (`get/put`) vor fi înregistrate în jurnal.

După ce utilizatorul s-a conectat la serverul intermediar și a fost afișat mesajul de întâmpinare, dacă ați creat un astfel de mesaj, este afișat promptul `ftp>`. Așa cum puteți vedea în figura 14.3, la acest prompt utilizatorul trebuie să lanseze comanda `user` pentru a specifica gazda la care vrea să se conecteze. Formatul comenzii este următorul:

```
user username@hostname
```

unde `username` este un nume valid de utilizator pentru gazda `hostname`, care este calculatorul cu care serverul intermediar FTP va realiza conexiunea.

De exemplu, pentru ca un utilizator de la distanță să obțină sau să stocheze fișiere pe un server numit `karma`, sub numele `smithj`, trebuie să folosească mai întâi clientul FTP pentru stabilirea unei sesiuni cu serverul intermediar de pe firewall, apoi să specifice serverul cu care vrea să interacționeze, cu ajutorul următoarelor comenzi:

```
popeye> ftp firewall.ono.com
Connected to firewall.ono.com
[mesaj de intampinare si asa mai departe]
ftp> user smithj@karma
```

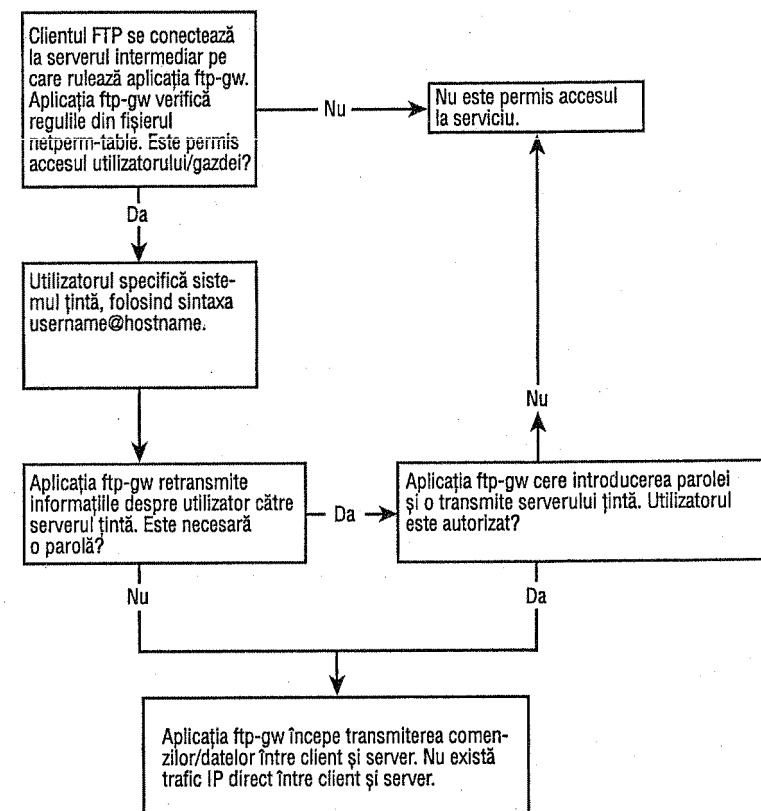
După ce realizează o conexiune cu gazda `karma` și îi transmite numele de utilizator `smithj`, aplicația intermediar îi cere utilizatorului să introducă parola pentru numele `smithj`.

Nu uitați că aceasta este o aplicație intermediar. Ca urmare, utilizatorul de la distanță nu poate trimite niciodată un pachet IP de pe calculatorul propriu către calculatorul gazdă specificat în comanda `user`. Serverul intermediar primește cererile (și toate pachetele IP) de la sistemul aflat la distanță și apoi, la nivelul aplicației, interacționează cu situl FTP destinat în locul utilizatorului de la distanță.

Acest proces în două etape poate părea complicat, dar pasul în plus nu înseamnă nimic în comparație cu securitatea pe care serverul intermediar o poate asigura rețelei.

FIGURA 14.3

Aplicația `ftp-gw` retransmite informațiile între client și serverul FTP țintă.



Conectările de la distanță și Telnet: `tn-gw` și `rlogin-gw`

Serverul intermediar `tn-gw` funcționează într-o manieră asemănătoare cu aplicația `ftp-gw`. Configurați aplicația folosind cuvinte cheie similare pentru atribute în fișierul `netperm-table`. De fapt, folosiți aceleași cuvinte cheie pentru configurarea aplicației `tn-gw` ca și pentru aplicația `ftp-gw` (prezentate în secțiunea anterioară, în tabelul 14.3), dar există și două cuvinte cheie suplimentare. Tabelul 14.5 prezintă cuvintele cheie suplimentare pe care le puteți folosi pentru aplicația intermediar `tn-gw`.

Tabelul 14.5 Cuvintele cheie pentru atributele de configurare folosite împreună cu aplicația intermediar tn-gw

Cuvânt cheie	Descriere
Prompt <i>prompt</i>	Folosiți acest cuvânt cheie pentru a specifica promptul prezentat utilizatorului de serverul intermediar Telnet atunci când este folosit în linie de comandă. Dacă folosiți un prompt care conține spații, de obicei este nevoie să plasați textul între ghilimele.
<i>Xforwarder program</i>	Folosiți acest cuvânt cheie pentru a specifica unde se află programul executabil către care aplicația intermediar Telnet va retransmite cererile pentru serverul intermediar X. În cele mai multe cazuri, aici este precizat locul unde se află serverul intermediar X.

Opțiunile pe care le puteți folosi cu cuvântul cheie `hosts` sunt mai puține decât în cazul aplicației `ftp-gw`. Evident, unele dintre cuvintele cheie folosite pentru aplicația intermediar FTP, cum ar fi `-log operatie`, sunt specifice protocolului FTP. Telnet nu are un set de operații pe care le poate executa. Acesta nu asigură decât o sesiune de terminal la distanță între utilizatorul aflat la distanță și sistemul țintă.

Opțiunea `-dest` funcționează la fel ca și în cazul aplicației `ftp-gw`. Folosiți această opțiune pentru a specifica una sau mai multe destinații la care este permis accesul. Nu uitați că este permisă folosirea caracterelor de înlocuire, iar caracterul „!” poate fi folosit pentru negarea unei destinații.

Două alte opțiuni pot fi folosite cu atributul `hosts`:

- `-auth` Folosiți această opțiune pentru a preciza că utilizatorul trebuie să se autentifice cu un identificator și o parolă valide înainte de a putea folosi poarta.
- `-passok` Folosiți această opțiune pentru a preciza că utilizatorul își poate schimba parola (atunci când se conectează de la o gazdă căreia i se aplică regula respectivă).

După ce s-a conectat la serverul intermediar Telnet, utilizatorul poate folosi comanda `connect` pentru a realiza o conexiune cu o anumită gazdă. Și în acest caz, rețineți că nu există trafic IP direct între utilizatorul de la distanță și sistemul țintă. Serverul intermediar primește date de la utilizatorul aflat la distanță, apoi acționează în numele acestuia pentru a transmite cererile către demonul Telnet al sistemului țintă.

Tabelul 14.6 prezintă comenzile pe care utilizatorul le poate lansa după ce s-a conectat la serverul intermediar tn-gw.

Tabelul 14.6 Comenzi recunoscute de serverul intermediar tn-gw

Comanda	Descriere
<code>connect host [port]</code>	Conectează utilizatorul într-o sesiune Telnet la gazda specificată (și la un anumit port, dacă este specificat). Pentru argumentul <i>host</i> puteți folosi un nume de gazdă sau o adresă IP.
<code>exit</code> sau <code>quit</code>	Iese din serverul intermediar Telnet.

Comanda	Descriere
<code>Help</code> sau <code>?</code>	Afișează un text de ajutor.
<code>password</code>	Permite utilizatorului să-și schimbe parola de autentificare puternică. Acest lucru poate fi făcut numai de pe gazdele specificate în fișierul <code>netperm-table</code> .
<code>x-gw [hostname:display [.screennumber]]</code>	Această comandă apelează serverul intermediar X pentru conectarea utilizatorului la gazda sau displayul specificat.

Ca și serviciul Telnet, `rlogin` poate fi folosit pentru obținerea promptului de comandă al unui sistem de la distanță în vederea executării unor comenzi. Totuși, spre deosebire de Telnet, `rlogin` nu cere autentificarea utilizatorului pentru un serviciu care rulează pe un sistem de la distanță. Accesul este controlat prin folosirea fișierelor `hosts.equiv` și `.rhosts`. În funcție de fișierul folosit, accesul este permis dacă numele sau adresa IP a gazdei sau numele utilizatorului care face cererea se află în aceste fișiere.

Vezi și

- Pentru mai multe informații despre diferitele servicii „r” care folosesc fișierele `hosts.equiv` și `.rhosts` și motivele pentru care acestea reprezintă un risc din punctul de vedere al securității, vezi pagina 55.

Poarta intermediar `rlogin-gw` pe care o puteți compila din setul de instrumente este configurată aproape la fel ca și aplicația `tn-gw`. Cuvintele cheie pentru atribute și opțiunile sunt aceleași. De asemenea, setul de comenzi pe care le poate folosi utilizatorul după conectarea la serverul intermediar este același. Principala diferență dintre cele două este faptul că trebuie să configurați fișierele `hosts.equiv` și `.rhosts` de pe sistemul țintă astfel încât să acorde încredere gazdei firewall-ului, nu calculatorului de la distanță de pe care se conectează utilizatorul. Ca și în cazul aplicației intermediar `tn-gw`, prin regulile din fișierul `netperm-table` puteți specifica gazdele cărora li se permite să folosească aplicația intermediar. De asemenea, puteți impune ca utilizatorii să se autentifice pe firewall înainte de a li se permite să continue și să stabilească o sesiune la distanță pe calculatorul țintă.

Serviciile „r” au fost inițial proiectate pentru a evita transmiterea parolelor sub formă de text clar prin rețea. Din acest motiv sunt folosite fișierele `hosts.equiv` și `.rhosts`. Securitatea serviciilor se bazează pe capacitatea unui calculator de a acorda încredere unui alt calculator. Prin folosirea autentificării puternice împreună cu aplicația `rlogin-gw`, puteți evita interceptarea numelor de utilizatori și a parolelor în timpul autentificării utilizatorilor pe firewall. Totuși, deși aplicația intermediar din firewall vă poate proteja împotriva folosirii rău-intenționate a acestor servicii din afara rețelei protejate de firewall, nu uitați că firewall-ul nu poate face nimic împotriva utilizatorilor din rețeaua internă. În general, serviciile „r” nu sunt o soluție prea bună dacă aveți un număr mare de utilizatori, iar securitatea este un aspect important pentru rețeaua dumneavoastră.

SMTP: smap

Dintre toate programele folosite în mod nefast de-a lungul timpului, profitând de hibe cunoscute și de alte probleme de codare, unul dintre cele mai faimoase este sendmail. De exemplu, dacă programatorul nu verifică informațiile introduse de utilizator pentru a se asigura că datele încap în bufferul rezervat, este posibil să fie suprascris nu numai spațiul bufferului, ci și codul programului. Atunci când se întâmplă acest lucru, rezultatele sunt imprevizibile – de obicei, programul se va bloca în urma unui atac prin refuzarea serviciului. Sau, dacă atacatorul este puțin mai inteligent, ar putea fi executat codul suprascris în locul codului original. Deoarece sendmail rulează de obicei sub root, rezultatele pot fi dezastruoase, oferind codului executabil acces la întregul sistem.

Așa ceva s-a întâmplat cam cu zece ani în urmă, în cazul cunoscutului „vierme Internet” (Internet Worm), care a folosit programul sendmail pentru a compromite mii de sisteme într-un timp foarte scurt. De atunci, s-au făcut mai multe încercări de corectare a programului. Totuși, din cauza dimensiunii (mai mult de 20.000 de linii) și complexității, garantarea utilizării sigure a acestei aplicații poate fi dificilă. Un alt motiv pentru care sendmail (și alte programe de poștă electronică) pot prezenta o problemă de securitate este faptul că, de obicei, rulează cu permisiuni la nivel de sistem. Ca urmare, atunci când este exploatată o hibă, este posibil ca sistemul să rămână descoperit și protecția obișnuită a resurselor să nu mai fie o barieră.

Setul de instrumente asigură programe care sunt folosite pentru a face puțin mai sigură distribuirea mesajelor de poștă electronică. Acestea sunt smap și smapd. Atunci când folosiți aceste programe, nu este nevoie să faceți nici o modificare în programul de poștă electronică sau în fișierul de configurare al acestuia. În schimb, configurați programele smap și smapd, care retransmit traficul de poștă electronică între programul de poștă exterior și cel pe care îl folosiți în mod obișnuit în rețeaua internă.

Mecanismul de funcționare a acestor programe este foarte simplu. Programul client smap este lansat la încărcarea sistemului și ascultă portul SMTP (de obicei portul 25, conform definiției din fișierul /etc/services) pentru a primi cererile de poștă electronică. Dacă un mesaj de poștă electronică este livrat demonului smap, acesta nu încearcă să îl trimită către destinatar, ci îl scrie într-un director. Periodic, demonul smapd se trezește și verifică dacă în acest director există vreun fișier. În caz afirmativ, smapd apelează programul de poștă electronică, cum ar fi sendmail, care livrează mesajul către destinația finală. După ce mesajul a fost transmis către programul de poștă electronică, smapd îl șterge din directorul folosit pentru stocarea temporară.

Intercalând programele smap și smapd între programele de poștă electronică SMTP intern și extern, nu se mai realizează un contact direct prin firewall. Deși am menționat acest lucru de mai multe ori în cartea de față, cred că este important să subliniez din nou că programele intermediar smap și smapd nu pot face nimic pentru a vă proteja împotriva virusilor și a altor programe care pot fi trimise în sistemul dumneavoastră prin poșta electronică. Tot ce fac aceste programe este să blocheze folosirea greșită a programului sendmail (sau a unui alt program de poștă electronică) astfel încât acesta să nu poată fi exploatat în vederea compromiterii sistemului sau rețelei dumneavoastră.

Cuvintele cheie pentru atributele de configurare pe care le puteți folosi în fișierul netperm -table sunt prezentate în tabelul 14.7 pentru smap și în tabelul 14.8 pentru smapd.

Tabelul 14.7 Cuvintele cheie pentru atributele de configurare folosite cu aplicația client intermediar smap

Cuvânt cheie	Descriere
directory director	Folosit pentru specificarea directorului pe care îl va folosi smap ca director rădăcină înainte de a începe prelucrarea mesajelor de poștă electronică. De asemenea, acest director va fi folosit ca spațiu de stocare temporară pentru mesajele ce vor fi preluate de smapd.
groupid grup	Acest cuvânt cheie este folosit pentru a specifica numele grupului sub care va rula smap.
timeout secunde	Numărul de secunde care pot trece fără activitate înainte ca aplicația intermediar să fie deconectată.
userid utilizator	Acest cuvânt cheie este folosit pentru a specifica identificadorul de utilizator sub care va rula smap.

Tabelul 14.8 Cuvintele cheie pentru atributele de configurare folosite cu aplicația server intermediar smapd

Cuvânt cheie	Descriere
badadmin utilizator	Dacă smapd nu poate livra un mesaj, îl transmite către utilizatorul specificat cu ajutorul acestui cuvânt cheie. Valoarea specificată poate fi un nume de utilizator sau un pseudonim (alias).
baddir director	Dacă smapd nu poate livra mesajele, le stochează în directorul specificat cu ajutorul acestui cuvânt cheie. Directorul ar trebui să se afle pe același dispozitiv ca și directorul de derulare (specificat de cuvântul cheie directory) și ar trebui să aibă același proprietar și aceleași permisiuni ca și directorul de derulare.
directory director	Folosit pentru specificarea directorului pe care îl va folosi smapd ca director rădăcină înainte de a începe prelucrarea mesajelor de poștă electronică. De asemenea, acest director va fi folosit ca spațiu de stocare temporară pentru mesajele ce vor fi preluate de smapd.
executable program	Acesta este un cuvânt cheie obligatoriu și este folosit pentru a specifica numele programului smapd. Pentru livrarea mesajelor către programul de poștă electronică, smapd se va bifurca ¹ și va executa o copie a codului propriu pentru fiecare mesaj pe care îl manipulează.
groupid grup	Acest cuvânt cheie este folosit pentru a specifica numele grupului sub care va rula smapd.

continuare

¹ Procesul părinte smapd execută comenzile fork și exec pentru inițierea unui proces copil (n. trad.)

Tabelul 14.8 Continuare

Cuvânt cheie	Descriere
<code>maxchildren copii</code>	Folosiți acest cuvânt cheie pentru a specifica numărul maxim de procese copil (descendenți) pe care <code>smagd</code> le creează atunci când manipulează mesaje.
<code>sendmail program</code>	Folosit pentru specificarea căii de acces la programul de poștă electronică utilizat în interiorul rețelei.
<code>wakeup secunde</code>	Folosiți acest cuvânt cheie pentru a specifica durata în secunde a intervalului în care serverul <code>smagd</code> „doarme” înainte de a verifica dacă există mesaje în directorul de derulare. Dacă acest cuvânt cheie nu este folosit, durata prestabilită este de 60 de secunde.
<code>userid utilizator</code>	Acest cuvânt cheie este folosit pentru a specifica identificadorul de utilizator sub care va rula <code>smagd</code> .

În timp ce toate celelalte aplicații intermediar din setul de instrumente pot fi rulate prin fișierul `inetd.conf` pentru fiecare conexiune, aceste două programe trebuie să fie tratate puțin diferit. Programul client `smagd` trebuie să fie lansat la încărcarea sistemului. Acest lucru este făcut, de obicei, prin plasarea unei linii de cod în fișierul `/etc/rc.local`. De exemplu:

```
/usr/local/etc/smagd
```

Și aplicația server `smagd` poate fi lansată în acest mod, la fel ca toate celelalte aplicații intermediar, exceptând cazul în care aveți o versiune veche a setului de instrumente.

Configurarea firewall-ului în DNS pentru manipularea poștei electronice

Nu uitați să verificați configurația DNS din domeniul dumneavoastră, pentru a vă asigura că există o înregistrare MX (mail exchanger) care trimite traficul SMTP către firewall-ul pe care este rulat `smag`. Pentru mai multe informații despre DNS, vezi capitolul 2, „Introducere în suita de protocoale TCP/IP”.

Configurarea altor servicii: *plug-gw*

Dacă doriți să manipulați servicii pentru care setul de instrumente nu conține aplicații intermediar (cum ar fi NNTP – Network News Transport Protocol), puteți folosi programul intermediar `plug-gw`. Spre deosebire de celelalte aplicații intermediar din setul de instrumente, `plug-gw` nu are comenzi interne ce pot fi folosite pentru un anumit serviciu. De exemplu, aplicația intermediar `tn-gw` permite utilizatorului să lanseze comanda `connect` pentru a se conecta la un server de la distanță din rețeaua internă după ce a fost autentificat de firewall. În cazul utilizării programului `plug-gw`, nu este asigurat decât un „canal” care poate fi folosit pentru conectarea unei surse externe la o sursă internă, astfel încât un serviciu să poată fi trecut printr-un tunel creat în firewall. Securitatea asigurată de `plug-gw` constă în blocarea traficului direct prin firewall, adică tocmai ceea ce face o aplicație intermediar. Securitatea suplimentară este asigurată prin faptul că `plug-gw`, la fel ca și celelalte aplicații

intermediar din set, înregistrează în jurnal operațiile efectuate, așa că puteți verifica ulterior ce tip de trafic a fost transferat prin firewall. Schimbând date la nivelul aplicației, `plug-gw` nu face decât să conecteze cele două capete ale canalului de date.

Pentru fiecare serviciu pe care vreți să îl folosiți prin `plug-gw`, este creat un proces demon separat. Puteți configura programul `plug-gw` astfel încât să fie lansat din fișierul `inetd.conf` la detectarea unei conexiuni sau să fie lansat din fișierul `/etc/rc.local`. Pentru a permite demonului `inetd` să lanseze aplicația intermediar, creați o înregistrare asemănătoare cu cea de mai jos:

```
nntp      stream      tcp      nowait    root      /usr/local/etc/plug-gw
➔ plug-gw 119
```

În acest exemplu, aplicația intermediar `plug-gw` este folosită pentru tratarea cererilor adresate grupurilor de discuții din Internet. Dacă vă uitați în fișierul `/etc/services` veți vedea că 119 (ultimul element al înregistrării) este numărul de port pentru NNTP. Această valoare este transmisă împreună cu numele `plug-gw` ca argumente ale aplicației `plug-gw`. Așa cum ați văzut în tabelul 14.1, primul câmp al acestei înregistrări este numele serviciului pe care demonul `inetd` trebuie să îl lanseze ca răspuns la o încercare de realizare a unei conexiuni. De asemenea, rețineți că `inetd` știe numai numărul portului pentru care este făcută cererea, nu și numele serviciului. Fișierul `/etc/services` este folosit ca o referință încrucișată pentru porturi și numele de servicii asociate cu acestea.

Dacă decideți să rulați aplicația `plug-gw` ca demon, puteți folosi două argumente în linia de comandă pentru lansarea aplicației:

- `-daemon port [sau nume serviciu]`
- `-version`

Primul argument este folosit pentru a specifica portul sau serviciul pentru care `plug-gw` execută funcții de intermediere, în timp ce al doilea argument determină transmiterea la ieșirea standard a unor informații despre versiunea aplicației intermediar.

La fel ca toate celelalte aplicații din setul de instrumente, `plug-gw` poate fi configurată cu ajutorul fișierului `netperm-table`. Tabelul 14.9 prezintă cuvintele cheie ce pot fi folosite pentru atribute.

Tabelul 14.9 Cuvintele cheie pentru atributele de configurare folosite cu aplicația `plug-gw`

Cuvânt cheie	Descriere
<code>groupid grup</code>	Acest cuvânt cheie este folosit pentru a specifica numele grupului sub care va rula aplicația intermediar.
<code>port portid gazde</code>	Folosiți acest cuvânt cheie pentru a specifica numărul de port al serviciului și o listă a gazdelor care pot folosi serviciul.
<code>timeout secunde</code>	Intervalul de timp în care aplicația poate rămâne în așteptare înainte de a se deconecta.
<code>userid utilizator</code>	Acest cuvânt cheie este folosit pentru a specifica identificadorul de utilizator sub care va rula aplicația intermediar.

Pe lângă aceste cuvinte cheie pentru attribute, există și câteva opțiuni pe care trebuie să le folosiți pentru a specifica modul în care plug-gw încearcă să realizeze o conexiune. Aceste opțiuni sunt:

- **-plug-to gazda** Această opțiune este folosită pentru a indica gazda din rețeaua internă la care plug-gw va conecta cererea de serviciu primită. Această opțiune este obligatorie.
- **-privport** Folosiți această opțiune pentru a preciza că gazda care asigură serviciul folosește un număr de port rezervat. De obicei, această opțiune este folosită pentru creșterea securității.
- **-port portid** Această opțiune este folosită pentru specificarea numărului de port al gazdei interne. Dacă nu specificați această opțiune, va fi folosit în mod prestabilit numărul de port al cererii. Această opțiune este foarte utilă dacă vreți să rulați mai multe instanțe ale aplicației plug-gw pentru manipularea unor copii ale aceluiași serviciu. De exemplu, dacă rețeaua dumneavoastră trebuie să se conecteze la mai multe surse de informare externe, puteți configura fiecare gazdă de informare internă astfel încât să folosească un alt port. Dacă folosiți același port, plug-gw va încerca să conecteze toate serverele interne la aceeași gazdă de informare externă.

Haideți să vedem un exemplu de înregistrare din fișierul netperm-table pentru aplicația plug-gw:

```
plug-gw: port 119 140.176.115.* -plug-to 198.2.43.122
```

Această înregistrare simplă face ca toate calculatoarele gazdă din rețeaua 140.176.115.0 să se conecteze la o sursă externă de informare care folosește adresa IP 198.2.43.122. Remarcați că după identificatorul plug-gw: de la începutul liniei este specificat numărul portului (119) folosit pentru identificarea serviciului. Nu uitați că, în timp ce alte aplicații intermediar din setul de instrumente sunt dedicate unor servicii specifice, plug-gw este un serviciu și protocol neutru, așa că trebuie să îi comunicați serviciul pentru care manipulează cererile. Deoarece nu a fost folosită opțiunea -port după adresa gazdei, la sfârșitul liniei, portul prestabilit (119) este folosit și pentru conexiunea externă.

Să vedem încă două exemple de configurare:

```
plug-gw: port 2119 140.176.115.* -plug-to 198.2.43.122 -port 119
```

```
plug-gw: port 2120 140.176.115.* -plug-to 198.2.43.122 -port 119
```

În aceste cazuri a fost folosită opțiunea -port. De ce? Deoarece altfel ar fi fost folosite porturile prestabilite 2119 și 2120, care nu sunt valide pentru serverele de informare din Internet. Cele două exemple vă arată cum puteți configura aplicația intermediar astfel încât să folosiți două surse de informare externe pentru a asigura servicii de informare clienților din rețeaua internă. În acest caz, trebuie să configurați clienții să folosească unul dintre porturile 2119 și 2120, în funcție de serverul extern la care vreți să se conecteze. De asemenea, rețineți că la configurarea clienților pentru serviciile de informare folosiți adresa IP a firewall-ului, nu adresa serverului de informare extern, deoarece calculatoarele client ar trebui să se conecteze la firewall, care apoi retransmite cererile către serverul extern.

Dacă folosiți această metodă pentru lansarea mai multor instanțe ale programului plug-gw, asigurând servicii pe mai multe porturi, trebuie să vă asigurați că fișierul /etc/services conține înregistrări pentru fiecare dintre noile porturi. Pentru exemplele de mai sus, trebuie să adăugați următoarele linii:

```
nntp-a 2119/tcp readnews untp # Internet news server NNTP
```

```
nntp-B 2120/tcp readnews untp # Internet news server NNTP
```

De asemenea, trebuie să creați două intrări în fișierul inetd.conf, astfel încât demonul inetd să răspundă la cererile primite pe aceste porturi folosind programul plug-gw:

```
nntp-a stream tcp nowait root /usr/local/etc/plug-gw
```

```
→plug-gw 2119
```

```
nntp-b stream tcp nowait root /usr/local/etc/plug-gw
```

```
→plug-gw 2120
```

În sfârșit, rețineți că deși plug-gw poate fi un instrument util pentru asigurarea serviciilor de intermediere pentru multe tipuri de servicii, nu este întotdeauna o idee bună folosirea acestuia fără discriminare. Permanent sunt dezvoltate și apar în Internet noi servicii și protocoale. Ar trebui să rețineți că un firewall este construit pe baza politicii de securitate a sitului dumneavoastră. Nu adăugați pur și simplu noi servicii la firewall de fiecare dată când un utilizator face o cerere, gândindu-vă că serverul intermediar va împiedica apariția problemelor. Mai întâi trebuie să înțelegeți cum funcționează serviciul sau protocolul. Apoi, în funcție de importanța serviciului pentru utilizator, luați o decizie. Evaluați riscurile! Comparați-le cu beneficiile ce pot fi obținute!

Alte componente ale setului de instrumente FWTK

Pe lângă serviciile de intermediere prezentate în acest capitol, setul de instrumente oferă și servicii de autentificare, un înlocuitor pentru demonul UNIX syslogd și câteva instrumente pe care le puteți folosi pentru a testa securitatea sistemului.

Serviciul authd, de exemplu, poate fi configurat pentru a lucra împreună cu ftp-gw și tn-gw asigurând astfel o securitate suplimentară, obligând utilizatorii să se autentifice pe firewall înainte de a putea folosi serviciile. Serviciul authd poate fi configurat pentru a funcționa împreună cu diferite servicii de autentificare folosite deja pe scară largă.

Versiunea din setul de instrumente a demonului syslogd este o variantă extinsă a programului obișnuit, dar vă permite să specificați modele de căutare în fișierul de configurare și să apelați diferite programe atunci când apare un anumit eveniment. Ca urmare, puteți urmări în timp real evenimentele transmise de demonul syslogd. În loc să stați în fața unui terminal și să așteptați mesaje, puteți să configurați programul syslogd astfel încât acesta să oprească sistemul în cazul unei încălcări grave a regulilor de securitate.

Instalarea setului de instrumente pe o gazdă bastion

Setul de instrumente este distribuit sub formă de cod sursă și este scris în limbajul de programare C. Ca urmare, după ce ați descărcat setul de instrumente, trebuie să îl compilați pe sistemul local pentru a putea să îl folosiți. În pachetul de descărcare veți găsi câteva fișiere read-me pe care ar trebui să le citiți înainte de a începe. Înainte de a compila componentele setului de instrumente, citiți îndrumările disponibile la adresa www.fwtk.org pentru a vedea exemple specifice variantei UNIX pe care o aveți. De asemenea, puteți să vă înscrieți în lista poștală dedicată setului FWTK. În acest scop,

trimiteți la adresa `majordomo@ex.tis.com` un mesaj e-mail care să nu conțină decât textul „subscribe fwtk-users”.

Nu uitați că firewall-ul pe care îl construiți nu poate fi mai sigur decât gazda pe care rulează. De obicei, acest calculator este numit gazdă bastion.

Vezi și

- În *capitolul 6*, „Utilizarea unei gazde bastion” (pagina 112), am discutat mult despre cum puteți să protejați un sistem pentru a fi folosit în acest scop. Subiectele prezentate au acoperit un domeniu larg, de la limitarea serviciilor care rulează în sistem și eliminarea conturilor de utilizator inutile, la dezactivarea retransmiterii IP și reconstruirea nucleului.

Nu este de ajuns să instalați setul de instrumente pe un sistem UNIX nou ca să obțineți un firewall sigur. Citiți mai întâi *capitolul 6*!

Rezumat

Trusted Information Systems Internet Firewall Toolkit este un set gratuit de componente ce pot fi folosite pentru construirea unui firewall pe un sistem UNIX sigur, aflat în perimetrul rețelei dumneavoastră. Aceste instrumente vă permit să creați un firewall care asigură toate serviciile de rețea standard, cum ar fi Telnet, FTP și e-mail. În plus, aplicația intermediar plug-gw ajută la conectarea aplicațiilor client și server prin firewall atunci când nu există o aplicație intermediar standard.

Setul FWTK nu este un instrument care poate fi folosit de oricine. Numai un administrator UNIX experimentat, cunoscând bine suita TCP/IP, ar trebui să încerce folosirea componentelor setului pentru protejarea unei rețele. Serverul intermediar vă permite să configurați fiecare serviciu acceptat de firewall. Dacă nu cunoașteți serviciile de rețea asigurate de suita TCP/IP și modul în care acestea sunt configurate într-un sistem UNIX tipic, vă va fi dificil să folosiți setul de instrumente pentru crearea unui firewall în care să aveți încredere.

Deoarece setul de instrumente este susținut numai de alți utilizatori, nu vă puteți baza pe un furnizor atunci când aveți nevoie de ajutor. Nu uitați acest lucru atunci când trebuie să decideți dacă acest firewall este cea mai bună soluție pentru dumneavoastră.

Capitolul 15

SOCKS

- **SOCKS V4 și SOCKS V5**
- Aplicații „SOCKSificate”
- SOCKSCap
- Cum puteți obține protocolul SOCKS
- Asistență tehnică pentru SOCKS

SOCKS V4 și SOCKS V5

SOCKS este un protocol ce poate fi folosit pentru crearea conexiunilor de intermediere printr-un firewall. Dezvoltat inițial de David Koblas și Ying-Da Lee la NEC Systems Laboratory, SOCKS a fost standardizat printr-un număr mare de documente RFC (Request For Comments) și este folosit pe scară largă în Internet. Protocolul SOCKS poate fi folosit pentru a permite unei gazde aflate de o parte a serverului SOCKS să interacționeze cu o gazdă aflată de cealaltă parte, în urma autentificării, fără să aibă loc un transfer direct de pachete IP între cele două gazde.

Documentele RFC (Request For Comments) pentru SOCKS

De la versiunea 5, SOCKS a fost discutat în mai multe documente RFC. Dacă vreți să aflați mai multe despre modul de lucru al protocolului SOCKS, acesta este un punct de plecare foarte bun. Puteți descărca copii ale următoarelor documente RFC din situl Web NEC dedicat protocolului SOCKS, www.socks.nec.com:

RFC 1928, „Protocolul SOCKS, versiunea 5”¹, stabilește elementele de bază ale protocolului și descrie diferențele față de versiunea 4.

RFC 1929, „Autentificarea prin nume de utilizator și parolă pentru SOCKS V5”², descrie o metodă de folosire a numelor de utilizatori și parolelor sub formă de text clar pentru protocolul SOCKS.

RFC 1961, „Autentificarea GSSAPI pentru SOCKS V5”³, descrie o metodă mai sigură de autentificare ce poate fi folosită pentru protocolul SOCKS.

În plus, în situl Web NEC puteți găsi alte documente preliminare (Internet Drafts) care descriu diverse aspecte ale protocolului și implementării acestuia. De asemenea, există o serie de documente preliminare ce descriu versiunea 4 a protocolului.

¹ RFC 1928, „SOCKS Protocol Version 5” (n. trad.)

² RFC 1929, „Username/Password Authentication for SOCKS V5” (n. trad.)

³ RFC 1961, „GSSAPI Authentication for SOCKS V5” (n. trad.)

Nu uitați că SOCKS este un protocol. Depinde de furnizor dacă un anumit firewall acceptă serverul SOCKS. Produsele software client care acceptă conexiuni SOCKS sunt disponibile pe scară largă. Pentru aplicațiile mai vechi, NEC oferă mai multe soluții, inclusiv o bibliotecă de funcții ce pot fi folosite pentru „SOCKSificarea”¹ aplicației prin recompilare și o bibliotecă DLL pentru sistemele Windows, numită SocksCap, care poate intercepta apelurile către funcțiile de rețea WinSock.

Dacă vă interesează tehnologia, puteți descărca din situl NEC versiuni de referință ale protocolului SOCKS, împreună cu câteva utilitare client care folosesc acest protocol.

Versiunea 4

SOCKS este un protocol simplu. În V4, protocolul are trei funcții principale:

- Schimbul de cereri de conexiuni
- Configurarea circuitului intermediar
- Retransmiterea datelor aplicației

Aceste etape simple permit clientului să configureze prin serverul SOCKS un circuit care poate fi folosit pentru transmiterea traficului TCP de rețea al aplicației.

Cererea CONNECT

Pentru crearea unei conexiuni, aplicația client transmite o cerere CONNECT către serverul SOCKS. Această cerere conține mai multe câmpuri:

- **Numărul versiunii** Acest câmp de 8 biți conține numărul de versiune, care pentru această versiune este 4.
- **Codul de comandă SOCKS** Acest câmp de 8 biți este folosit pentru un cod care indică funcția pachetului. Valoarea 1 indică o cerere de conectare.
- **Portul destinație** Acest câmp de 16 biți este numărul portului de pe serverul țintă la care vrea să se conecteze clientul.
- **Adresa IP a destinației** Acest câmp de 32 de biți este adresa IP a serverului țintă la care vrea să se conecteze clientul.
- **Identificatorul utilizatorului (userID)** Acesta este un câmp de lungime variabilă care conține un identificator de utilizator valabil pentru serverul țintă.

După ce consultă fișierul de reguli și determină dacă este permisă conexiunea, serverul SOCKS încearcă să se conecteze la serverul țintă, folosind adresa IP și numărul de port furnizate de client. După ce această operație reușește (sau eșuează), serverul SOCKS returnează clientului un pachet care conține următoarele câmpuri:

- **Numărul versiunii** Acest câmp de 8 biți conține numărul de versiune al codului de răspuns și ar trebui să fie 0.
- **Codul rezultat SOCKS** Valoarea din acest câmp de 8 biți indică succesul sau eșecul operației de conectare.

¹ În original, *SOCKSifying*, un termen inventat pentru a descrie adăugarea funcțiilor SOCKS la un program existent (n. trad.)

De unde vine numele SOCKS?

Numele SOCKS nu a fost ales prin tragere la sorți, ci este o prescurtare a numelui folosit intern pe durata dezvoltării: SOCK-et-S (socluri).

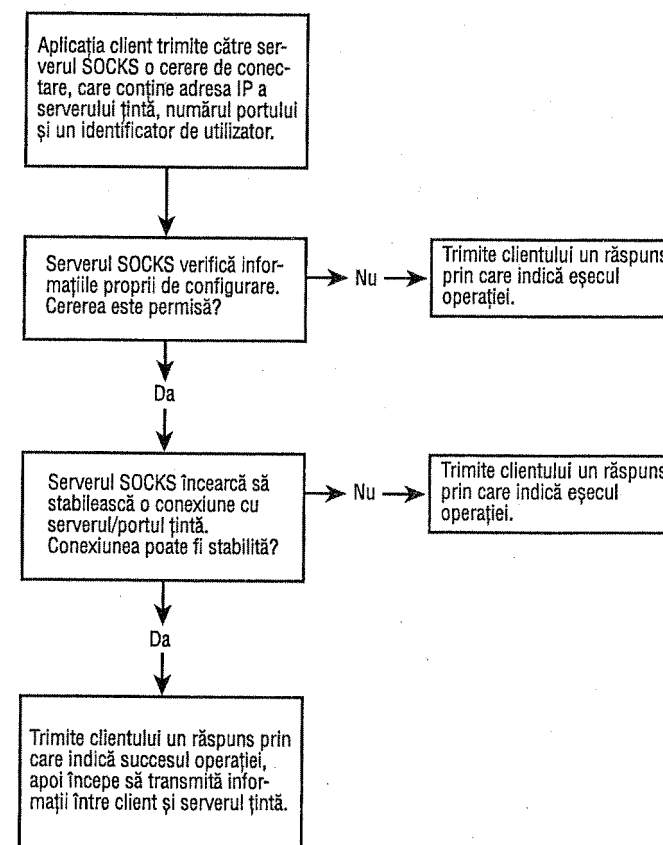
Cum este configurat un server SOCKS?

SOCKS este un protocol. Producătorii pot să implementeze detaliile de configurare cum doresc. SOCKS V5 Reference Implementation de la firma NEC, de exemplu, folosește un fișier de configurare numit `/etc/socks5.conf` pe server și `/etc/libsocks5.conf` pe client. Verificați documentația firewall-ului dumneavoastră pentru a vedea dacă acesta acceptă protocolul SOCKS.

Dacă mesajul conține un cod de eroare, serverul SOCKS termină conexiunea cu clientul după ce trimite acest răspuns. În caz contrar, serverul este gata să transmită date între aplicațiile client și server (vezi figura 15.1).

FIGURA 15.1

Pentru o cerere de conectare, un server SOCKS trebuie să verifice configurația proprie înainte de a se conecta la serverul țintă.



Cererea BIND

După ce o aplicație client a folosit cu succes cererea CONNECT pentru a stabili o conexiune intermediată cu o aplicație server țintă, cererea BIND poate fi folosită pentru a informa serverul SOCKS că clientul vrea să stabilească o conexiune de recepție cu serverul de aplicații. Conținutul cererii BIND este asemănător cu cel al cererii CONNECT, exceptând faptul că valoarea câmpului pentru codul de comandă SOCKS trebuie să fie 2. Dacă serverul SOCKS, după consultarea regulilor, decide că o asemenea conexiune este permisă, returnează clientului un pachet de răspuns asemănător cu cel trimis în cazul cererii CONNECT. Serverul SOCKS alocă un soclu la care vor fi primite pachetele de la serverul de aplicații și returnează aplicației client un răspuns care conține două câmpuri suplimentare:

- **Portul destinație** Acesta este portul alocat pe serverul SOCKS pentru primirea datelor de la serverul de aplicații.
- **Adresa IP a destinației** Aceasta este adresa IP a adaptorului de rețea de pe serverul SOCKS prin care sunt recepționate datele de la serverul de aplicații. Acest câmp este necesar dacă serverul SOCKS are mai multe adaptoare de rețea. Dacă valoarea acestui câmp este 0, clientul folosește aceeași adresă ca și conexiunea CONNECT originală cu serverul SOCKS.

Aplicația client folosește aceste informații despre soclu pentru a forma o cerere către serverul de aplicații țintă. Serverul de aplicații deschide apoi o conexiune cu serverul SOCKS, folosind acest soclu. Serverul SOCKS verifică dacă cea de-a doua conexiune provine de la aceeași gazdă cu cea identificată în cererea BIND originală și, în caz afirmativ, trimite aplicației client un alt pachet de răspuns, prin care o informează că a fost stabilită conexiunea (vezi figura 15.2).

Așa cum puteți vedea, deși protocolul SOCKS poate fi folosit pentru crearea unei conexiuni client/server prin firewall, protocolul în sine nu execută nici o verificare specifică aplicației. În acest mod, protocolul funcționează asemănător cu un filtru de pachete. Serverul SOCKS poate fi configurat astfel încât să permită sau să interzică accesul unor gazde sau rețele, dar nu intră în detalii privind permiterea anumitor funcții ale unei aplicații. Această funcționalitate intră în responsabilitatea aplicației codate în vederea utilizării protocolului SOCKS. Totuși, spre deosebire de un filtru de pachete, SOCKS nu transmite direct pachete între aplicațiile client și server. Între cele două nu există nici o conexiune directă.

Versiunea 5

Cea mai nouă versiune a protocolului SOCKS adaugă la TCP suportul pentru autentificare și pentru crearea serverelor intermediar UDP. De asemenea, noile specificații prevăd acceptarea numelor de domenii și adresarea IPv6.

Vezi și

- Pentru mai multe informații despre IPv6, următoarea generație a protocolului IP, vezi capitolul 21, „Firewall-uri și mai mult decât atât”, în pagina 306.

Porți la nivel de circuit

Multe servere intermediar folosesc aplicații intermediar specifice unui anumit protocol sau serviciu de rețea. De exemplu, o aplicație server intermediar poate fi folosită pentru FTP, în timp ce alta este folosită pentru Telnet. Aceste tipuri de aplicații intermediar nu sunt interschimbabile și pot fi folosite pentru a limita funcțiile serviciului la care are acces utilizatorul. Acest tip de server intermediar creează o poartă la nivel de aplicație între client și server.

Deoarece protocolul SOCKS nu înțelege aplicația client, ci doar asigură autentificarea și retransmiterea informațiilor, este considerat a fi o poartă la nivel de circuit, nu o poartă la nivel de aplicație.

În SOCKS V4, atunci când aplicația client trimitea o cerere CONNECT, în cerere era inclus și un identificator de utilizator. Această informație este folosită de serverul SOCKS atunci când consultă regulile pentru a decide dacă o conexiune poate fi permisă. SOCKS poate folosi și funcționalitatea protocolului IDENT pentru a verifica numele de utilizator al clientului care face cererea. Totuși, autentificarea propriu-zisă prin conexiunea intermediată nu este afectată de SOCKS V4. Ca urmare, dacă folosiți protocolul FTP printr-o conexiune SOCKS și clientul trimite numele de utilizator și parola sub formă de text clar, securitatea este compromisă dacă textul este interceptat.

SOCKS V5 adaugă acceptarea metodelor de autentificare într-o manieră generalizată, folosind un cadru de lucru de specificații, prin care asigură folosirea unor protocoale arbitrare de autentificare la configurarea inițială a conexiunii SOCKS.

După ce se conectează la serverul SOCKS, clientul trimite un mesaj care identifică versiunea protocolului SOCKS și una sau mai multe „metode” ce pot fi folosite pentru autentificare. Deși formatul pachetului permite până la 255 de metode diferite, în acest moment sunt definite doar câteva. Serverul SOCKS selectează una dintre metodele furnizate de client și returnează un mesaj prin care comunică clientului metoda aleasă. Valorile pentru metode sunt controlate de organizația IANA (Internet Assigned Numbers Authority) și în prezent sunt următoarele:

- Nu este necesară autentificarea (0)
- GSS-API (1)
- USERNAME/PASSWORD (2)
- IANA (3-127)
- Rezervate pentru metode private (128-254)
- Fără metode acceptabile (255)

După ce clientul a recepționat acest mesaj, clientul și serverul SOCKS intră într-o fază de negociere specifică metodei de autentificare aleasă.

Metodele de autentificare SOCKS V5

Alte două documente RFC detaliază două dintre metodele pe care protocolul SOCKS V5 le poate folosi pentru autentificare. Acestea sunt:

RFC 1929, „Autentificarea prin nume de utilizator și parolă pentru SOCKS V5”¹, descrie o metodă de autentificare ce folosește text clar pentru schimburile de informații referitoare la numele de utilizator și parolă, nefiind o metodă sigură.

¹ RFC 1929, „Username/Password Authentication for SOCKS V5” (n. trad.)

RFC 1961, „Autentificarea GSS-API pentru SOCKS V5”¹, descrie folosirea interfeței GSS-API pentru autentificare și în alte scopuri, cum ar fi încapsularea traficului IP. Interfața GSS-API este prezentată cu mai multe detalii în documentele RFC 1508 și 1509.

Formatul de cerere al protocolului SOCKS V5

Deși este asemănător cu formatul V4, formatul SOCKS V5 prevede includerea mai multor informații. Câmpul pentru numărul versiunii trebuie să conțină valoarea 5. Câmpul pentru comanda SOCKS poate avea trei valori:

- 1 CONNECT
- 2 BIND
- 3 UDP ASSOCIATE

Un nou câmp este folosit pentru a indica tipul adresei IP. Această valoare pe 8 biți ar trebui să fie 1 dacă adresa este de tip IPv4, 3 dacă adresa conține un nume de domeniu și 4 dacă adresa este de tip IPv6. Câmpul pentru portul destinație este același ca în versiunea 4, indicând portul țintă pentru serviciul la care vrea să se conecteze clientul. Dimensiunea câmpului pentru adresa destinației depinde de tipul adresei. Dacă este folosit un nume complet de domeniu, primul octet al câmpului de adresă (8 biți) conține o valoare ce indică lungimea (în octeți) a numelui de domeniu care urmează în câmpul de adresă.

Funcția UDP ASSOCIATE

Și în acest caz, câmpul pentru versiune al mesajului de răspuns are valoarea 5 în loc de 4. Câmpul pentru codul rezultat SOCKS poate conține aceleași valori ca în versiunea 4, plus alte câteva. De asemenea, mesajul de răspuns conține câmpuri pentru adresă și tipul adresei, ca și în formatul de cerere.

Pe lângă cererile CONNECT și BIND, SOCKS V5 oferă un nou serviciu, care permite crearea serverelor intermediar UDP. În pachetul de cerere UDP ASSOCIATE, clientul comunică serverului portul și adresa IP pe care vrea să le folosească pentru asociere. Pachetul de răspuns returnat de server comunică clientului numărul portului și adresa IP la care acesta trebuie să trimită pachetele pentru conexiune. Retransmiterea traficului UDP se face altfel decât în cazul traficului TCP. În loc să recepționeze pur și simplu pachete dintr-o parte a conexiunii și să le retransmită către cealaltă parte, fiecare pachet pe care serverul SOCKS îl primește de la client are atașat un antet de cerere UDP. Acest antet de cerere include câmpurile standard folosite pentru cererile/răspunsurile SOCKS, precum și portul și adresa IP ale destinației.

Deoarece UDP este un protocol fără conexiune, nefiabil, și nu asigură confirmarea primirii pachetelor, serverul SOCKS nu informează clientul dacă pachetul a fost retransmis sau abandonat.

Fragmentarea UDP

Protocolul SOCKS V5 conține în antetul de cerere un câmp care poate fi folosit pentru a indica dacă un pachet a fost fragmentat. Aceasta este o caracteristică opțională și poate să nu fie implementată de toate serverele.

¹ RFC 1961, „GSSAPI Authentication for SOCKS V5” (n. trad.)

Aplicații „SOCKSificate”

Dacă aveți codul sursă pentru o aplicație care nu acceptă încă protocolul SOCKS, uneori este posibil să o „SOCKSificați”, recompilând-o cu o bibliotecă de funcții furnizate de NEC împreună cu versiunea SOCKS V5 Reference Implementation. Biblioteca include rutine care, funcțional, sunt echivalente cu funcțiile de soclu BSD standard, dar implementează protocolul SOCKS.

În situl Web NEC SOCKS puteți găsi informații detaliate privind modificările minore pe care trebuie să le faceți în codul existent și modul de legare a codului cu funcțiile de bibliotecă SOCKS. Iată adresa URL pentru această legătură: www.socks.nec.com/how2socksify.html

SocksCap

Interfața SocksCap poate fi folosită în sistemele Windows pentru a permite aplicațiilor să lucreze prin firewall-ul SOCKS fără modificări în aplicația originală. SocksCap interceptează apelurile făcute către serviciile de rețea de clienți WinSock și le trimite către serverul SOCKS. Există mai multe versiuni ale interfeței SocksCap, atât pe 16, cât și pe 32 de biți. Pentru Windows 95 și Windows 98, puteți folosi oricare dintre cele două versiuni, în funcție de aplicațiile client folosite cu serverul SOCKS. Sub Windows NT pot fi folosite numai versiunile pe 32 de biți.

Rețineți că SocksCap nu înlocuiește interfața WinSock, ci doar schimbă o parte din funcționalitatea acesteia.

Pentru descărcarea interfeței SocksCap, vizitați următorul sit Web: www.socks.nec.com

Cum puteți obține protocolul SOCKS

În situl Web NEC puteți găsi o mulțime de informații despre protocoalele SOCKS. În privința aplicațiilor client, dacă aveți dubii puteți întreba producătorul, dar cele mai multe aplicații sunt distribuite cu suport integrat pentru SOCKS. Dacă aplicația pe care vreți să o folosiți nu poate lucra cu serverul intermediar SOCKS, există câteva soluții, cum ar fi „SOCKSificarea” aplicației prin recompilare, așa cum am menționat anterior, folosirea interfeței SocksCap sau implementarea unei alte soluții bazate pe o bibliotecă SOCKS.

De asemenea, cele mai multe firewall-uri importante acceptă protocolul SOCKS. Dacă autentificarea puternică este importantă pentru securitatea sitului dumneavoastră – așa cum ar trebui să fie – consultați documentația pentru a verifica dacă produsul se bazează pe SOCKS V4 sau V5.

Pe lângă implementările comerciale ale protocolului SOCKS, NEC permite descărcarea versiunii SOCKS V5 Reference Implementation. Aceasta este furnizată în cod sursă și poate fi descărcată de la următoarea adresă: ftp.nec.com/pub/socks/socks5

Acest pachet conține și aplicații client pentru Telnet, FTP, finger, whois, archie, ping și traceroute.

Există și o implementare creată de Hewlett-Packard pentru uz intern. Puteți descărca acest server SOCKS de la următoarea adresă: <ftp.cup.hp.com/disk/socks>

Asistență tehnică pentru SOCKS

Ar trebui să puteți obține asistență tehnică pentru orice firewall bun de la producătorul acestuia. Totuși, asistența tehnică este probabil limitată la aspecte de configurare și rezolvarea problemelor minore. Dacă vreți să aprofundați studierea aspectelor tehnice ale protocolului SOCKS sau să rămâneți la curent cu noile dezvoltări legate de protocol și de aplicațiile bazate pe acesta, există trei liste poștale cu specific SOCKS la care vă puteți înscrie. Pentru înscriere, trimiteți un mesaj e-mail la adresa majordomo@socks.nec.com. Nu folosiți linia de subiect a mesajului, ci includeți un text asemănător cu cel de mai jos în corpul mesajului:

Subscribe <lista> dumneavoastra@adresa.com

unde *lista* este lista la care vreți să vă înscrieți (SOCKS, SOCKS5 sau SOCKSCAP).

Rezumat

Protocolul SOCKS este un exemplu privind modul în care sunt dezvoltate noi protocoale și servicii ca răspuns la creșterea rapidă a Internetului. Pe măsură ce cresc cerințele de securitate, un cadru de lucru precum SOCKS poate fi folosit de mai mulți producători pentru crearea unor aplicații ce conlucrează într-o manieră standardizată. În următorul capitol veți analiza un alt server intermediar disponibil în Internet: SQUID, un server intermediar al cărui principal obiectiv este intermedierea prin cache.

Capitolul 16

SQUID

- Ce este SQUID?
- Cum puteți obține serverul SQUID
- Instalarea și configurarea serverului SQUID
- Gestionarea serverului SQUID
- Configurarea clienților pentru folosirea serverului SQUID

Ce este SQUID?

SQUID este un server intermediar cu cache. Dacă vă mai amintiți, una dintre primele utilizări ale unui server intermediar era păstrarea în cache a paginilor Web vizitate frecvent, ceea ce permitea economisirea capacității de transfer. Aceasta se întâmplă mai ales la începutul Internetului, atunci când nu existau prea multe situri comerciale. Deoarece Internetul era folosit în mare parte în scopuri științifice și educaționale, mulți utilizatori foloseau aceeași sursă de informații, descărcând aceleași informații la fiecare acces. Prin păstrarea pe un server local a datelor solicitate frecvent, în mare parte statice, un răspuns primit de la un sit Web putea fi folosit pentru a satisface mai mulți utilizatori locali.

Ce este GNU?

GNU este un sistem de operare de tip UNIX, dezvoltat, printre alții, de Richard Stallman, începând din 1983. Intenția acestora a fost să pună la dispoziție un sistem de operare gratuit, împreună cu codul sursă, pe care utilizatorii îl pot rula și modifica. Organizația Free Software Foundation a fost înființată pentru a sprijini dezvoltarea ulterioară a produselor software deschise și gratuite. Pentru mai multe informații despre ceea ce puteți și ce nu puteți face cu produsele software acoperite de licența GNU, vizitați situl Web Free Software Foundation, la adresa www.fsf.org.

Serverele intermediare cu cache funcționează prin păstrarea unor copii ale obiectelor obținute recent din Internet într-un cache de pe discul local sau din memorie. Dacă după puțin timp este primită o altă cerere pentru același obiect, serverul intermediar poate folosi copia locală a datelor, în loc să trimită o altă cerere către adresa URL originală a obiectului.

Serverul intermediar SQUID este disponibil gratuit în Internet, sub licență GNU. Deși SQUID poate fi descărcat gratuit din Internet, nu trebuie considerat un produs simplu, cu un set redus de funcții. SQUID are un set bogat de caracteristici și poate fi folosit în rețele de diferite mărimi pentru asigurarea serviciilor de cache. Printre caracteristicile importante ale serverului SQUID se numără:

- Servicii de intermediere și de păstrare în cache pentru protocoalele HTTP, FTP și SSL.

- Organizare ierarhică, ceea ce permite mai multor servere de cache să fie configurate pentru a lucra împreună, folosind protocolul standard ICP (Internet Caching Protocol).
- Operare transparentă pentru utilizatori.
- Controlul accesului.
- Păstrarea în cache a căutărilor DNS.
- Accelerarea serverului HTTP.

SQUID este un produs complex, cu multe opțiuni de configurare. În acest capitol vom discuta pe scurt despre instalarea, pornirea și rularea serverului SQUID folosind valorile de configurare prestabilite. Dacă vreți să evaluați serverul SQUID în vederea utilizării acestuia într-un firewall, ar fi bine să studiați documentele SQUID FAQ, pentru a înțelege mai bine comenzile complexe de configurare ce pot fi folosite pentru gestionarea serverului SQUID.

Cum puteți obține serverul SQUID

Dacă vreți să descărcați serverul SQUID, puteți vizita situl Web SQUID. Dacă aveți sistemul de operare Linux, este bine să verificați mai întâi documentația sistemului. Multe variante de Linux conțin codul sursă SQUID, iar unele includ chiar și codul binar compilat. Totuși, în situl Web, veți găsi lista SQUID FAQ oficială, un ghid de utilizare și documentație ce poate fi de folos oricui vrea să folosească serverul SQUID într-un sistem productiv. Ca urmare, chiar dacă aveți deja în sistem serverul SQUID, situl Web oficial poate fi o resursă valoroasă. Adresa URL a sitului SQUID este:

www.squid-cache.org.

În momentul publicării acestei cărți¹, cea mai recentă versiune a serverului SQUID era 2.3. Totuși, pot fi descărcate și versiuni anterioare.

Instalarea și configurarea serverului SQUID

Pentru instalarea serverului SQUID, este bine ca mai întâi să creați un cont de utilizator sub care va rula serverul intermediar. Nu instalați și nu rulați serverul SQUID sub root. Singurele fișiere la care trebuie să aibă acces SQUID sunt fișierele proprii de configurare și fișierele și directoarele folosite pentru stocarea obiectelor de cache. Practica recomandată este să creați un cont de utilizator squid și un director (/usr/local/squid) pentru cont, apoi să folosiți acest cont pentru rularea serverului SQUID. Atunci când despachetați fișierul tar² și compilați codul sursă al serverului SQUID, folosiți contul squid, pentru ca acesta să devină proprietarul fișierelor create.

¹ Ediția originală a apărut în iunie 2000 (n. trad.)

² Utilitar UNIX de arhivare care permite stocarea fără comprimare a mai multor fișiere într-unul singur, cu extensia .tar. Despachetarea fișierului se face cu utilitarul untar (n. trad.)

Alegerea unui server SQUID

Atunci când stabiliți serverul care va fi folosit pentru instalarea programelor SQUID, alegeți un sistem care are destulă memorie și un sistem de discuri eficient. Deoarece păstrarea în cache implică stocarea pe termen scurt a obiectelor descărcate din Internet, folosirea mai multor discuri pentru directoarele de cache SQUID îmbunătățește performanțele. Viteza UCP nu influențează performanțele la fel de mult ca și cantitatea de memorie. Cu cât vă puteți permite mai multă memorie, cu atât mai rapide vor fi răspunsurile primite de utilizatori. Se recomandă ca serverul SQUID să aibă cel puțin 128 MB de memorie, dar este mai bine să aibă 256 MB sau mai mult.

Ce sistem de operare ar trebui să folosiți pentru SQUID

Deși multe variante de Linux includ codul sursă pentru SQUID, nu este obligatoriu să folosiți o platformă Linux. Serverul SQUID poate fi rulat cu succes pe platforme AIX, FreeBSD, HP-UX, Irix, NetBSD, Nextstep, SCO și Solaris.

Instalarea componentelor software

Instalarea serverului SQUID este o problemă simplă. După ce creați contul de utilizator sub care va rula SQUID, vă conectați la contul respectiv, executați câteva comenzi pentru compilarea codului și creați directoarele și indecșii pe care îi va folosi SQUID.

Instalarea serverului SQUID

1. Creați un director pentru stocarea fișierelor sursă SQUID:

```
# mkdir -p /usr/local/squid/src
```

2. Alegeți ca director prestabilit directorul pe care tocmai l-ați creat și despachetați fișierele comprimate care conțin sursa SQUID:

```
# gzip -cd squid-s.3.STABLE2-src.tar.gz | tar xv
```

Această comandă creează și câteva subdirectoare. Directorul /doc conține, desigur, informații utile și ar trebui să citiți aceste fișiere, în special fișierele readme care conțin informații despre actualizări și modificări recente.

3. Folosiți comanda configure pentru a lansa un proces automatizat de verificare a serverului:

```
# ./configure
```

4. Folosiți fișierul make SQUID pentru compilarea codului sursă și, după terminarea cu succes a compilării, folosiți parametrul install pentru a instala serverul SQUID:

```
# make
```

```
# make install
```

Aceste comenzi vor instala serverul SQUID în mai multe directoare ce vor fi create sub directorul /usr/local/squid, inclusiv subdirectoarele bin, etc, cache și logs.

5. Este creată o copie prestabilită a fișierului de configurare /usr/local/squid/etc/squid.conf. Puteți să folosiți această copie a fișierului sau să folosiți un editor de texte pentru a modifica înregistrările din fișier. De exemplu, dacă nu vreți să stocați

obiectele de cache în directorul prestabilit `/usr/local/squid/cache`, ci pe un alt disc, puteți edita fișierul de configurare pentru a modifica această înregistrare.

6. Folosiți comanda `squid` pentru crearea directoarelor folosite pentru indexarea datelor stocate:

```
# /usr/local/bin/squid -z
```

7. În sfârșit, folosiți comanda `squid` pentru a lansa un proces de fundal care recepționează cereri prin portul prestabilit al serverului SQUID, respectiv 3128. Verificați fișierul jurnal `/usr/local/bin/logs/cache.log` pentru a vedea dacă au apărut erori.

Utilizarea scriptului `configure`

În exemplul care vă arată cum să compilați fișierele SQUID, ați remarcat că trebuie să rulați scriptul `configure` după ce decompilați fișierele, dar înainte de a le compila. Scriptul `configure`, printre altele, evaluează sistemul și creează fișierele `make`. Acest fișier script primește mai mulți parametri, care pot fi folosiți pentru a-i controla modul de funcționare. De exemplu, puteți cere scriptului `configure` să folosească un alt director decât `/usr/local/squid`. Pentru a afla mai multe despre parametrii pe care îi puteți folosi cu scriptul de configurare, introduceți comanda `./configure-help`.

Dacă este executată fără nici un parametru, comanda `squid` lansează un proces părinte, care apoi creează un proces copil. Procesul copil este cel care îndeplinește, de fapt, funcțiile programului. Dacă, dintr-un motiv oarecare, procesul copil își termină execuția, procesul părinte generează un nou proces copil. Puteți verifica fișierul de mesaje `syslog` dacă doriți să vedeți înregistrările create de SQUID atunci când pornește sau repornește un proces. Dacă observați că acest lucru se întâmplă foarte des, verificați fișierul jurnal al serverului SQUID, numit `cache.log`, pentru a încerca să rezolvați problema.

Pentru a determina dacă serverul SQUID funcționează așa cum vă așteptați, configurați un client, cum ar fi Internet Explorer, să folosească serverul SQUID, apoi încercați să răsfoiți paginile din Web. După ce vă convingeți că totul merge bine, adăugați o comandă în fișierele de pornire a sistemului, astfel încât serverul SQUID să fie lansat la încărcarea sistemului.

Gestionarea serverului SQUID

Pentru a face modificări în configurația curentă a serverului SQUID, trebuie să editați fișierul de configurare, apoi să apelați comanda `squid` pentru a aplica modificările. După ce editați fișierul `squid.conf`, folosiți următoarea comandă pentru a aplica modificările efectuate:

```
/usr/local/bin/squid -k reconfigure
```

Fișierul `squid.conf`

Acesta este principalul fișier de configurare pentru SQUID și, de obicei, se află în directorul `/usr/local/squid/etc/`. Acest fișier conține diferite informații, cum ar fi portul HTTP folosit de SQUID. Nu trebuie să vă faceți probleme privind crearea acestui fișier pornind de la zero. Atunci când executați scriptul `configure`, comanda `make install` creează automat o copie prestabilită a acestui fișier. Parametrii pe care îi puteți modifica în

fișier sunt numeroși și cel mai bun mod de a începe este să citiți fișierul de la un capăt la altul. Fișierul prestabilit creat la instalare conține multe comentarii și, ca urmare, cea mai mare parte a comenzilor din fișier sunt ușor de urmărit. Înainte de a începe să faceți modificări în acest fișier, vă sugerez să citiți documentele SQUID FAQ, care sunt actualizate mai des decât ghidul de utilizare. Pe lângă răspunsurile la întrebări referitoare la configurarea serverului SQUID cu ajutorul acestui fișier, veți afla și cum puteți să configurați listele de control al accesului (ACL – Access Control Lists), care stabilesc la ce obiecte este permis accesul sau ce utilizatori și gazde pot să folosească serverul SQUID.

Fișierul prestabilit `squid.conf` poate fi păstrat ca atare dacă vreți să folosiți serverul SQUID numai pentru cache și nu vreți să controlați accesul utilizatorilor sau accesul la adresele URL. Documentele SQUID FAQ pot fi descărcate din situl Web SQUID, de la adresa www.squid-cache.org.

Comanda `squid`

Pentru pornirea serverului de cache SQUID, nu trebuie decât să lansați comanda `squid`. Totuși, sintaxa acestei comenzi este destul de complicată. După ce vă familiarizați cu folosirea comenzii `squid`, puteți încerca să faceți și alte lucruri. Câțiva dintre cei mai importanți parametri în linie de comandă pentru comanda `squid` sunt:

- **-a port** Cere serverului SQUID să folosească un alt port pentru recepționarea cererilor HTTP. Valoarea prestabilită este 3128.
- **-d nivel de eroare** Stabilește nivelul la care sunt trimise mesaje de depanare către `stderr`.
- **-f** Stabilește un alt fișier de configurare în locul fișierului `squid.conf`.
- **-h** Afișează informații de ajutor.
- **-k reconfigure** Trimite serverului SQUID semnalul HUP, cerându-i să citească din nou fișierul de configurare.
- **-k rotate** Trimite serverului SQUID semnalul USR1. În urma acestui semnal, serverul SQUID rotește fișierele de jurnal (închide fișierul curent, îl redenumeste și deschide un nou fișier).
- **-k shutdown** Trimite serverului SQUID un semnal TERM, cerându-i să se oprească. Înainte de a se opri, serverul SQUID așteaptă o scurtă perioadă de timp, pentru a permite închiderea conexiunilor curente.
- **-k interrupt** Trimite serverului SQUID un semnal INT, cerându-i să se oprească imediat.
- **-k kill** Trimite serverului SQUID un semnal KILL. În urma acestui semnal, serverul SQUID se oprește fără să execute nici o operație de „curățare” a fișierelor. Această comandă ar trebui folosită numai dacă nu merge nimic altceva.
- **-k debug** Trimite serverului SQUID semnalul USR2. Până la primirea următorului semnal USR2, SQUID generează mesaje de depanare completă.
- **-k check** Trimite serverului SQUID un semnal ZERO pentru a verifica dacă procesul rulează. Verificați variabilele de stare de ieșire ale nucleului dacă vreți să aflați rezultatele.

- **-s** Cere serverului SQUID să transmită către syslog numai mesaje de depanare de nivel 0.
- **-u** Folosit pentru a specifica un alt număr de port pentru recepționarea mesajelor ICP. Valoarea prestabilită este 3130.
- **-v** Cere serverului SQUID să afișeze numărul versiunii.
- **-z** Folosit pentru crearea directoarelor de schimb.
- **-D** Suprimă testarea DNS. Dacă nu este folosit acest parametru, SQUID încearcă să verifice la pornire câteva nume de gazde recunoscute, pentru a vedea dacă serverul DNS funcționează corespunzător.
- **-F** Folosit pentru reconstruirea cache-ului în „prim-plan”. În acest mod, cache-ul este reconstruit mai rapid, dar cererile HTTP nu sunt servite în această perioadă.
- **-N** Cere serverului SQUID să nu ruleze ca proces de fundal. Acest parametru este util pentru testare, dacă vreți ca procesul să ruleze pe terminalul dumneavoastră.
- **-R** Cere serverului SQUID să nu activeze opțiunea SO_REUSEADDR pentru socluri.
- **-V** Acest parametru activează acceptarea gazdelor virtuale pentru modul httpd-accelerator.
- **-X** Cere serverului SQUID să folosească modul de depanare completă atunci când citește fișierul de configurare.
- **-Y** Folosiți acest parametru pentru a permite reconstruirea mai rapidă a cache-ului, atunci când sunt folosite în principal cache-uri copil.

Mulți dintre acești parametri sunt utili pentru depanare și probabil nu vor fi folosiți niciodată de administratorii obișnuiți ai serverului SQUID. Comenzile pe care este cel mai probabil să le folosiți sunt cele simple, cum ar fi `squid`, pentru lansarea aplicației. Uneori vreți să știți dacă serverul SQUID mai rulează. Pentru aceasta, introduceți următoarea comandă:

```
# squid -k check
```

După ce executați această comandă, verificați variabilele de stare ale nucleului pe care îl folosiți, pentru a vedea dacă a apărut o eventuală eroare. Pentru a rula serverul SQUID în prim-plan, în vederea depanării, folosiți următoarea comandă:

```
# squid -N
```

Jurnalele SQUID

SQUID folosește mai multe fișiere jurnal. Acestea sunt:

- **cache.log** Acest fișier conține informații legate chiar de serverul SQUID, inclusiv mesaje de eroare generale și informații despre pornirea și oprirea serverului.
- **access.log** Acest fișier înregistrează cererile făcute de clienți către serverul SQUID. Analizând acest fișier puteți determina care sunt cele mai populare situri Web vizitate de clienții dumneavoastră.
- **store.log** Acest fișier urmărește datele adăugate sau scoase din cache. Deoarece acest fișier poate deveni destul de mare, puteți să îl dezactivați. Pentru a face acest lucru, adăugați în fișierul `squid.conf` comanda `cache_store_log none`.

- **swap.log** Acest fișier înregistrează informații despre fiecare obiect de cache scris pe disc, cum ar fi fișierul în care este păstrat obiectul și o marcă de timp ce indică momentul în care obiectul a fost verificat ultima dată ca actual. SQUID citește din nou acest fișier jurnal la pornire.

Datele din aceste fișiere sunt destul de ușor de înțeles. De exemplu, fișierul `access.log` acceptă un format nativ, dar poate folosi și formatul standard CERN pentru înregistrarea în jurnal a cererilor de acces HTTP. Codurile de stare HTTP folosite în toate jurnalele sunt cele definite în documentul RFC 2068. Pe lângă fișierul `cache.log`, SQUID trimite mesaje de jurnal și către `syslogd`. Atunci când depanați probleme legate de server, verificați atât fișierul `cache.log`, cât și fișierele jurnal păstrate de `syslogd`.

Jurnalele păstrate de SQUID pot deveni destul de mari și ar trebui să le verificați periodic. Pentru gestionarea jurnalelor mari, *rotiți-le* și salvați vechile fișiere off-line. Pentru rotirea fișierelor jurnal, folosiți următoarea comandă:

```
# squid -k rotate
```

Atunci când folosiți această comandă, SQUID închide fișierele jurnal, le redenumeste cu o extensie numerică (de exemplu, `.0` sau `.1`) și deschide un nou fișier. După ce vă obișnuieți cu volumul de date colectate în aceste fișiere, puteți automatiza procesul, prin crearea unui program cron.

Analiza jurnalelor SQUID

Jurnalele produse de SQUID pot ajunge foarte mari, ceea ce face dificilă interpretarea datelor pe care le conțin. De exemplu, citirea fișierului `access.log` pentru localizarea accesului unui anumit utilizator la un anumit sit Web poate fi o sarcină oșitoare dacă fișierul este mare. În situl Web SQUID puteți găsi legături către aplicații pe care alții le-au dezvoltat pentru a simplifica analiza datelor produse de SQUID.

Ce este protocolul ICP (Internet Cache Protocol)?

Acest protocol este folosit de serverele intermediar cu cache pentru a comunica unul cu celălalt. Documentul RFC 2186, „Internet Cache Protocol (ICP) versiunea 2”, descrie standardul pentru versiunea 2 a protocolului ICP. În acest document veți găsi informații despre formatul folosit pentru mesaje. Dacă vreți să aflați mai multe despre funcționarea protocolului ICP, citiți și documentul RFC 2187, „Aplicații ale protocolului ICP (Internet Cache Protocol) versiunea 2”¹. Acest document RFC nu se oprește la formatul mesajelor, ci descrie și modul în care serverele folosesc protocolul pentru lansarea cererilor și răspunsurilor sau pentru obținerea obiectelor din cache-urile vecine.

Ce este ierarhia de cache SQUID?

SQUID poate lucra ca server intermediar independent sau puteți folosi mai multe servere SQUID, configurate prin relații părinte-copil. Folosirea unei structuri ierarhice de servere SQUID poate fi mai eficientă pentru un sit mare decât folosirea unui singur server SQUID.

În ierarhia de cache, puteți găsi atât servere de cache părinte, cât și servere copil (rude). Un server SQUID poate interoga atât un server părinte, cât și un server de pe același nivel al ierarhiei, atunci când are nevoie de un obiect care nu se află în cache-ul propriu.

Serverul încearcă mai întâi să obțină obiectul solicitat căutând în cache-ul propriu. Dacă nu găsește obiectul, trimite interogări UDP către serverele pe care le cunoaște ca rude.

¹ RFC 2187, „Application of Internet Cache Protocol (ICP) Version 2” (n. trad.)

Dacă nici unul dintre acestea nu îi poate furniza o copie a obiectului, serverul ia legătura cu serverul părinte din ierarhie, dacă există. Dacă nici acesta nu deține o copie a obiectului, părintele obține obiectul din Web și returnează o copie serverului copil care l-a solicitat. După cum vedeți, interacțiunea cu rudele de pe același nivel și cu părinții este asemănătoare, dar nu identică. Deși un server SQUID poate cere o copie a obiectului atât de la serverele rude, cât și de la serverul părinte, numai serverul părinte încearcă să obțină obiectul din Web, dacă nu deține deja o copie a acestuia. Dacă serverele rude nu dețin o copie a obiectului, nu fac decât să returneze un mesaj.

Pentru a configura un server să folosească un server de cache părinte sau rudă, creați înregistrări în fișierul `squid.conf`. De exemplu:

```
cache_peer parent.twoinc.com parent 3128 3130
```

Această înregistrare îi comunică serverului SQUID că există un părinte, numit `parent.twoinc.com`, pe care îl poate folosi pentru cererile pe care el sau serverele rude nu le pot rezolva. La fel, puteți folosi următoarea înregistrare:

```
cache_peer child1.twoinc.com sibling 3128 3130
```

Această înregistrare îi comunică serverului SQUID că poate interoga un server copil (rudă), numit `child1.twoinc.com`, pentru obiectele pe care nu le are în cache-ul propriu.

Configurarea clienților pentru folosirea serverului SQUID

Cele mai multe browsere moderne pot să lucreze cu servere intermediar. De exemplu, ca să configurați browserul Internet Explorer pentru folosirea unui server SQUID pentru rezolvarea solicitărilor HTTP, FTP și gopher, parcurgeți următoarele etape:

Configurarea browserului Internet Explorer pentru folosirea serverului SQUID

1. Din Internet Explorer, executați clic pe meniul Tools, apoi selectați comanda Internet Options.
2. După ce apare caseta de dialog Internet Options, executați clic pe eticheta Connections, apoi pe butonul LAN Settings.
3. După ce apare caseta de dialog Local Area Network (LAN) Settings, executați clic pe butonul Advanced. Este afișată caseta de dialog Proxy Settings, care poate fi folosită pentru desemnarea serverelor intermediar.
4. Pentru fiecare protocol de rețea pe care vreți să îl folosească clientul pentru serverul SQUID, introduceți adresa IP sau numele DNS complet al serverului SQUID în rubrica etichetată Proxy Address to Use. În rubrica Port, introduceți numărul portului folosit de serverul SQUID pentru recepționarea cererilor (valoarea prestabilită este 3128).
5. Executați clic pe butonul OK din fiecare casetă de dialog ca să o închideți.

Configurarea browserului Netscape Navigator pentru folosirea serverului SQUID

1. Din Netscape Navigator, selectați opțiunea Network Preferences din meniul Edit.
2. Selectați opțiunea Advanced, apoi opțiunea Proxies, din meniul Category.
3. Selectați butonul radio etichetat Manual Proxy Configuration, apoi executați clic pe butonul View.

4. Pentru fiecare protocol de rețea pe care vreți să îl folosească clientul pentru serverul SQUID, introduceți adresa IP sau numele DNS complet al serverului SQUID în rubrica etichetată Proxy Address to Use. În rubrica Port, introduceți numărul portului folosit de serverul SQUID pentru recepționarea cererilor (valoarea prestabilită este 3128).

5. Executați clic pe butonul OK din fiecare casetă de dialog ca să o închideți.

Pentru a afla cum puteți să configurați un anumit produs, folosiți funcția de ajutor (help) și căutați cuvântul „proxy”. Dacă aplicația client nu știe să folosească servere intermediar, probabil că ar trebui să vă gândiți că este timpul să treceți la un produs mai nou!

Rezumat

SQUID este un server intermediar cu cache, gratuit, care rulează pe platforme UNIX (și Linux). SQUID poate fi folosit ca server independent sau în combinație cu alte servere SQUID, formând o ierarhie. Puteți folosi serverul SQUID și într-o ierarhie formată din servere de cache de alt tip, dacă acestea acceptă protocolul ICP. În următorul capitol veți vedea alte două aplicații ce pot fi obținute gratuit și care pot fi folosite pentru construirea unui firewall: `ipfwadm` și `ipchains`, rulate sub Linux.

Utilizarea programelor *ipfwadm* și *ipchains* sub Linux

- Ce sunt *ipfwadm* și *ipchains*?
- Instalarea și configurarea programului *ipfwadm*
- Instalarea și configurarea programului *ipchains*

Ce sunt *ipfwadm* și *ipchains*?

Sistemul de operare Linux include în nucleu funcții de filtrare a pachetelor. Programele *ipfwadm* și *ipchains* pot fi folosite pentru gestionarea firewall-ului și a regulilor pentru conturi, stabilite prin nucleu. Folosind aceste programe, puteți crea seturi de reguli pentru filtrarea pachetelor IP recepționate de calculatorul gazdă, transmise de acesta sau retransmise de la un adaptor de rețea al gazdei la altul. Fiecare regulă specifică anumite criterii, cum ar fi informațiile de adresare IP sau tipul protocolului, precum și o acțiune executată dacă un pachet îndeplinește criteriile regulii. De exemplu, în funcție de adresa IP, regulile pot fi configurate pentru acceptarea sau abandonarea unui pachet recepționat. Ca urmare, folosind un sistem Linux configurat ca gazdă bastion cu două plăci de rețea, puteți crea un filtru de pachete fără să suportați costul suplimentar al unor programe speciale sau al unui nou router.

Vezi și

➤ Pentru informații detaliate despre conceptele implicate de filtrarea pachetelor, vezi capitolul 5, „Filtrarea pachetelor”, la pagina 95.

Totuși, este bine să știți de la început că trebuie să fiți familiarizat cu administrarea sistemelor UNIX și protocolul TCP/IP pentru a folosi programele *ipfwadm* și *ipchains*. Compilarea și instalarea codului sursă nu reprezintă o sarcină dificilă, dar ar trebui să înțelegeți bine sintaxa complexă a acestor utilitare și să testați configurația înainte de a considera că eforturile făcute au avut succes.

În acest capitol veți afla sintaxa celor două utilitare și veți găsi câteva sugestii. Dacă urmează să folosiți programele *ipfwadm* și *ipchains*, vă recomand să vizitați diferitele situri Web dedicate acestora, pentru a analiza sugestiile și exemplele pe care le veți găsi. Nu uitați că Linux și produsele asociate sunt dezvoltate, în principal, într-un mediu deschis, iar asistența tehnică este disponibilă, de obicei, numai prin grupuri de discuții și liste poștale din Internet. Dacă folosiți o implementare comercială, precum Red Hat sau Caldera, verificați ce asistență poate oferi furnizorul înainte de a face din aceste programe o

componentă importantă a sistemului dumneavoastră de securitate. Puteți găsi informații despre Red Hat la adresa www.redhat.com, iar despre Caldera la adresa www.caldera.com.

Vezi și

➤ Filtrarea pachetelor nu este, în sine, o soluție adecvată pentru un firewall complet. Totuși, atunci când sunt combinate cu alte aplicații, cum ar fi Trusted Information Systems Internet Firewall Toolkit (FWTK), posibilitățile de filtrare a pachetelor oferite de nucleul Linux pot fi folosite pentru crearea unui firewall foarte bun. Pentru mai multe informații despre TIS FWTK, vezi capitolul 14, „Folosirea setului de instrumente FWTK (TIS Firewall Toolkit)”, la pagina 217.

Instalarea și configurarea programului *ipfwadm*

Primul utilitar pe care îl vom prezenta în acest capitol este *ipfwadm*. Acesta se bazează pe codul original *ipfw*, parte a sistemului de operare BSD UNIX.

Instalarea programului *ipfwadm* se reduce la obținerea codului sursă și folosirea fișierului *make* pentru compilarea și instalarea programului. Deși este ușor să obțineți codul sursă, instalarea și gestionarea acestuia nu reprezintă o problemă la fel de simplă. Cei mai mulți administratori Linux experimentați consideră acest proces destul de simplu. Probabil nu vi se va părea la fel dacă nu sunteți familiarizat cu sistemul de operare. Programul *ipfwadm* nu are o interfață grafică cu utilizatorul, așa că trebuie să învățați și să înțelegeți bine sintaxa comenzilor folosite pentru configurarea și gestionarea regulilor.

Obținerea programului *ipfwadm*

Puteți descărca fișierele de cod sursă pentru *ipfwadm*, precum și fișierele binare pentru unele sisteme, din paginile Web create de X/OS Experts in Open Systems BV:

<http://www.xos.nl/linux/ipfwadm/>

Pentru folosirea programului *ipfwadm*, trebuie să aveți un nucleu Linux versiunea 1.2.1 sau mai nou. Cea mai nouă versiune a programului *ipfwadm* este 2.3.0, iar aceasta funcționează doar cu nuclee Linux de la versiunea 1.3.66 la 2.0.36. Dacă aveți o versiune mai nouă a nucleului, trebuie să folosiți în schimb programul *ipchains*.

Caracteristicile pe care le puteți folosi dintr-o anumită versiune depind de versiunea nucleului Linux pe care o aveți. Consultați documentul *readme* din fișierele descărcate pentru a afla informații mai precise despre versiuni și caracteristicile disponibile pentru acestea.

Instalarea programului *ipfwadm*

După ce descărcați codul sursă, folosiți un utilitar de comprimare pentru despachetarea fișierelor. De exemplu:

```
gzip -c -d ipfwadm_2.3.0.tar.gz | tar xvf -
```

Apoi folosiți fișierul *make* pentru compilarea și instalarea programului. Specificați ca prestabilit directorul folosit pentru codul sursă și introduceți următoarele comenzi:


```
make ipfwadm
```

```
make install
```

Ultima comandă `make` creează următoarele directoare:

```
■ /sbin/ipfwadm
```

```
■ /usr/man/man8/ipfwadm.8
```

```
■ /usr/man/man4/ipfw.4
```

După această instalare simplă, trebuie să creați regulile, în funcție de politica de securitate a sitului dumneavoastră. Pentru crearea sau gestionarea regulilor, folosiți comanda `ipfwadm`.

Folosirea comenzilor `ipfwadm`

Există patru categorii de reguli pe care le puteți gestiona folosind comanda `ipfwadm`:

- **Firewall de intrare IP** Reguli pentru pachetele IP recepționate printr-o interfață de rețea
- **Firewall de ieșire IP** Reguli pentru pachetele IP transmise printr-o interfață de rețea
- **Firewall de retransmitere IP** Reguli pentru pachetele IP retransmise de la o interfață de rețea la alta
- **Contorizarea pachetelor IP** Reguli pentru selectarea pachetelor care vor incrementa contoarele de octeți

Filtrarea prin aceste reguli este permisă pentru protocoalele TCP, UDP și ICMP.

Vezi și

- *Ce sunt protocoalele TCP, UDP și ICMP? Pentru mai multe informații despre protocoalele de bază, vezi capitolul 2, „Introducere în suita de protocoale TCP/IP”, la pagina 26.*

Sintaxa comenzii `ipfwadm` este următoarea:

```
ipfwadm -categorie comanda parametri [optiuni]
```

Pentru *categorie* puteți folosi cinci parametri, care specifică setul de reguli asupra cărora este aplicată comanda. Aceștia sunt:

- **-A *directie*** Reguli de contorizare, unde *directie* este opțională și poate fi `in`, `out` sau `both`. Dacă nu este specificată o direcție, valoarea prestabilită este `both` (ambele direcții).
- **-I** Reguli pentru firewall de ieșire
- **-O** Reguli pentru firewall de intrare
- **-F** Reguli pentru firewall de retransmitere
- **-M** Gestionarea mascării IP. Această opțiune poate fi folosită cu `-l` pentru listarea informațiilor despre reguli sau cu `-s` pentru stabilirea duratelor de așteptare.

După *categorie*, trebuie să indicați o comandă, care specifică o acțiune ce va fi executată pentru categoria respectivă. Pot fi folosite următoarele comenzi:

- **-a *politica*** Folosiți această comandă pentru a adăuga una sau mai multe reguli la sfârșitul listei. În cazul înlănuirilor firewall, folosiți pentru *politica* una dintre următoarele valori: `accept`, `deny` sau `reject`. În cazul înlănuirilor de contorizare, nu folosiți nici o valoare pentru *politica*.

- **-i *politica*** Această comandă inserează una sau mai multe reguli în listă. Folosiți pentru *politica* aceleași valori ca și în cazul comenzii `-a`.
- **-d *politica*** Această comandă șterge una sau mai multe reguli din listă. Folosiți aceeași sintaxă ca și în cazul comenzilor `-a` sau `-i`. Prima regulă care corespunde sintaxei este ștersă.
- **-l** Această comandă listează toate regulile din listă.
- **-z** Această comandă reinițializează contoarele de octeți pentru toate regulile din listă. Puteți folosi împreună comenzile `-l` și `-z`. În acest caz, valorile contoarelor sunt aduse la zero după ce sunt afișate de comanda de listare.
- **-f** Această comandă șterge lista de reguli.
- **-p *politica*** Această comandă poate fi folosită pentru a schimba politica prestabilită pentru firewall-ul selectat. Și în acest caz, parametrul *politica* poate avea una dintre valorile: `accept`, `deny` sau `reject` și trebuie folosit numai cu regulile pentru firewall, nu și pentru contorizare. Politica prestabilită a unui firewall este folosită atunci când pentru un pachet nu se găsește o regulă specifică.
- **-s *tcp topfin udp*** Această comandă este folosită pentru modificarea duratelor de așteptare pentru mascare. Trebuie să folosiți toți cei trei parametri și să specificați valorile în secunde. Prima valoare (*tcp*) este durata de așteptare pentru sesiunile TCP, a doua (*topfin*) este durata de așteptare pentru sesiunile TCP care au primit un pachet FIN, iar a treia (*udp*) este durata de așteptare pentru pachetele UDP. Această comandă poate fi folosită numai cu categoria `-M`, pentru gestionarea mascării. Dacă vreți să schimbați duratele de așteptare numai pentru una sau două categorii, folosiți valori zero pentru categoriile pe care vreți să le lăsați nemodificate.
- **-c** Această comandă poate fi folosită pentru a verifica dacă un pachet IP a fost acceptat sau respins de reguli. Comanda poate fi folosită numai pentru categoriile `-I`, `-O` și `-F`.
- **-h** Aceasta este comanda de asistență (`help`).

Pentru aceste comenzi, puteți folosi parametrul *politica* (adică valorile `accept`, `reject` sau `deny`) numai cu categoriile pentru firewall-uri. Aceste valori nu sunt valabile pentru categoria de contorizare, deoarece comenzile corespunzătoare acestei categorii nu impun o politică, ci doar execută funcții de contorizare statistică. Așa cum ați văzut, comanda `-p politica` poate fi folosită pentru specificarea unei politici prestabilite pentru o anumită categorie de firewall. Această politică este folosită atunci când nici o regulă din categoria respectivă nu se poate aplica în cazul unui pachet evaluat. Ca urmare, puteți să stabiliți reguli specifice pentru situațiile pe care le cunoașteți și să folosiți politica prestabilită pentru respingerea (sau acceptarea) tuturor celorlalte pachete.

Diferența dintre `reject` și `deny`

În cazul pachetelor pe care nu vreți să le lăsați să treacă, puteți instrui programul `ipfwadm` să răspundă în două moduri. Pachetele pot fi respinse (`reject`) sau interzise (`deny`). Dacă într-o regulă folosiți politica `reject`, pachetele care nu sunt acceptate au ca rezultat trimiterea unui mesaj ICMP *host unreachable* către clientul care a transmis pachetele. Dacă folosiți politica `deny`, pachetele sunt abandonate, dar nu este trimis nici un mesaj către sursă.

Parametri

Atunci când gestionați reguli, le inserați, le adăugați sau le ștergeți. Pentru folosirea acestor comenzi, trebuie să specificați unele informații suplimentare, necesare pentru identificarea regulilor asupra cărora se acționează. Amintiți-vă sintaxa comenzii *ipfwadm*:

ipfwadm -categorie comanda parametri [optiuni]

Până acum am discutat despre categorii, care selectează lista de reguli ce urmează să fie gestionată, și despre comandă, care execută o acțiune asupra listei specificate. Pentru comenzile de inserare, adăugare și ștergere, puteți folosi următorii parametri:

- **-P protocol** Acest parametru poate avea valorile *tcp*, *udp*, *icmp* sau *all* și specifică protocolul pentru care va fi aplicată regula. Valoarea prestabilită este *all*. De exemplu, o regulă cu parametrul *-P tcp* este aplicată numai pachetelor TCP, în timp ce o regulă cu parametrul *-P udp* este aplicată numai pachetelor UDP.
- **-S adresa[/masca][port ...]** Acest parametru este folosit pentru specificarea sursei. Pentru *adresa*, specificați un nume de gazdă, un nume de rețea sau o adresă IP. Pentru *masca*, specificați o mască de rețea. Pentru *port*, specificați unul sau mai multe numere de porturi sau un tip ICMP pentru protocolul ICMP.
- **-D adresa[/masca][port ...]** Acest parametru este folosit pentru specificarea destinației. Sintaxa este aceeași ca și în cazul parametrului *-S*, exceptând faptul că nu puteți folosi tipuri ICMP pentru adresa destinației.
- **-V adresa** Acest parametru opțional este folosit pentru specificarea interfeței prin care este primit sau transmis pachetul. Pentru *adresa*, puteți folosi un nume de gazdă sau o adresă IP.
- **-W nume** Acest parametru opțional este folosit pentru a specifica numele interfeței prin care este primit sau transmis pachetul.

Opțiuni

În sfârșit, există o serie de opțiuni pe care le puteți folosi în linia de comandă pentru selectarea mai precisă a regulilor. Acestea sunt următoarele:

- **-b** Desemnează modul de lucru bidirecțional, ceea ce înseamnă că regula este aplicată pachetelor în ambele direcții.
- **-e** Această opțiune este folosită numai împreună cu comanda de listare și determină afișarea mai multor informații.
- **-k** Această opțiune este folosită pentru selectarea pachetelor care au bitul ACK activat. Opțiunea poate fi folosită numai împreună cu regulile pentru protocolul TCP.
- **-m** Această opțiune face ca pachetele acceptate pentru retransmisie să fie mascate cu adresa gazdei în locul adresei de la care provin.
- **-n** Această opțiune determină afișarea rezultatelor în format numeric, în loc de text, acolo unde este cazul. De exemplu, sunt afișate adresele IP în locul numelor de gazde.
- **-o** Această opțiune zactivează înregistrarea în jurnal de către nucleu a pachetelor care corespund regulii.
- **-r port** Această opțiune redirecționează pachetele către un soclu local.

- **-t andmask xormask** Această opțiune specifică o mască folosită pentru modificarea câmpului TOS din antetul IP.
- **-v** Această opțiune determină afișarea mai multor informații la ieșire.
- **-x** Această opțiune determină afișarea valorilor exacte ale contoarelor. În mod prestabilit, aceste numere sunt rotunjite la multipli de 1.000 (1K) sau multipli de 1000 K.
- **-y** Această opțiune determină aplicarea regulii asupra pachetelor TCP care au biții SIN și ACK șterși.

Ținând seama de această listă lungă de opțiuni, precum și de numeroasele comenzi pe care le puteți folosi pentru fiecare categorie, sintaxa comenzii *ipfwadm* poate părea greoaie. Totuși, după ce veți începe să experimentați folosirea comenzii, aceasta nu va mai părea atât de dificilă. Iată un exemplu:

```
ipfwadm -Fle
```

Această comandă va afișa (1 pentru listare) toate regulile pentru retransmitere (F) în format extins (e). Următoarele două comenzi afișează regulile pentru pachetele recepționate (I), respectiv transmise (O), folosind formatul extins (e) și prezentând adresele și numerele de porturi în format numeric (n):

```
ipfwadm -Inle
```

```
ipfwadm -Onle
```

Este o idee bună să creați reguli prin specificarea politicilor prestabilite pentru fiecare categorie de firewall. De exemplu, ca să specificați politica prestabilită pentru retransmiterea pachetelor IP, puteți folosi următoarea comandă:

```
ipfwadm -F -p deny
```

În acest caz, opțiunea *-p deny* precizează că politica prestabilită este de a interzice retransmiterea IP. În mod normal, un sistem Linux cu două adaptoare de rețea retransmite pachetele primite la un adaptor de rețea către celălalt adaptor de rețea, dacă acestea nu sunt destinate gazdei locale. Interzicerea retransmiterii prin politica prestabilită este o idee bună dacă folosiți gazda ca firewall. Nu uitați că, deși opțiunile *deny* și *reject* sunt similare, *reject* determină returnarea unui mesaj *icmp* către sursa pachetului. În cazul unui firewall cu securitate puternică, este mai bine să nu transmiteți nici un fel de informații.

Probabil că este o idee bună să mergeți și mai departe și să specificați opțiunea *deny* ca politică prestabilită pentru toate categoriile firewall-ului, înaintea oricărei alte reguli. Deoarece comanda *-p politica* precizează doar politica prestabilită, folosirea acestei comenzi la începutul fișierului nu determină respingerea imediată a tuturor pachetelor. Pachetul este respins numai dacă până la sfârșitul fișierului nu este găsită o altă regulă aplicabilă. Dacă doriți să specificați politica prestabilită pentru categoriile de intrare și de ieșire, înlocuiți în exemplul precedent *-F* cu *-I* sau *-O*.

După ce ați început prin a interzice accesul în mod prestabilit, puteți crea regulile care specifică gazdele care au dreptul să treacă prin fiecare interfață de rețea. Regulile pe care le construiți depind de adresele IP reale folosite în rețea și de conexiunea la Internet. Pentru un set bun de exemple, un document excelent este IPFWADM FAQ. Acest document FAQ poate fi găsit la următoarea adresă:

<http://www.dreamwvr.com/ipfwadm/ipfwadm-faq.html>

Plasarea regulilor pentru programul *ipfwadm* în fișierul de pornire

După ce ați creat lista de reguli pe care vreți să le folosiți, puteți să le plasați într-unul dintre fișierele de pornire, astfel încât regulile să intre în vigoare la încărcarea sistemului. De exemplu, puteți plasa regulile în fișierul `r.local`.

Instalarea și configurarea programului *ipchains*

Mai devreme în acest capitol, am menționat că programul *ipfwadm* funcționează numai cu nuclee Linux până la versiunea 2.0.36. Pentru nuclee Linux mai noi (versiunea 2.1.102 și cele mai recente), trebuie să folosiți utilitarul mai nou, *ipchains*. Acest utilitar este o versiune rescrisă a codului Linux pentru firewall-ul IP și a utilitarului *ipfwadm*. Rezultatul este un utilitar mai flexibil ce poate fi folosit pentru gestionarea filtrării pachetelor pe sistemele Linux. Pentru a vedea dacă versiunea Linux pe care o aveți asigură suportul de nucleu pentru noul utilitar de filtrare a pachetelor *ipchains*, căutați fișierul `/proc/net/ip_fwchains`. Dacă acest fișier există în sistemul dumneavoastră, sunteți gata de drum. Dacă nu, puteți vizita situl Web oficial *ipchains* pentru a verifica dacă există un program de corectare. Dacă nu există, va trebui să treceți la un nucleu Linux mai nou.

Obținerea programului *ipchains*

Puteți descărca programul *ipchains* din situl Web oficial dedicat acestuia:

www.rustcorp.com/linux/ipchains

Aici veți găsi codul sursă, precum și fișierele binare pentru câteva variante UNIX. De asemenea, veți găsi legături către mai multe versiuni ale documentului HOW-TO și instrucțiuni pentru abonarea la câteva liste poștale cu discuții despre programul *ipchains*.

Care sunt diferențele între *ipfwadm* și *ipchains*?

Așa cum *ipfwadm* a fost o îmbunătățire a utilitarului original *ipfw*, *ipchains* este o îmbunătățire a utilitarului *ipfwadm*. Cele două utilitare sunt similare, prin faptul că ambele sunt folosite pentru gestionarea listelor de reguli aplicate pachetelor IP dintr-un sistem gazdă. Totuși, există și unele diferențe:

- Sintaxa a fost îmbunătățită. În programul *ipchains*, literele mari sunt folosite pentru comenzi, iar literele mici sunt folosite pentru opțiuni.
- Pe lângă listele – sau înlanțuirile – interne de reguli, *ipchains* vă permite să creați și liste denumite de utilizatori. Prin crearea unor liste proprii de reguli, testarea configurațiilor este mai ușoară. Dacă faceți o greșală, nu trebuie decât să ștergeți (sau să modificați) lista pe care ați creat-o. Dacă manevrați continuu regulile dintr-una din listele interne, veți ajunge să vă încurcați și să uitați ce funcționa la început!

- A fost adăugat un operator care poate fi folosit pentru negarea unei valori (operatorul `!`).
- Prelucrarea fragmentelor de pachete a fost îmbunătățită.
- Lista de reguli pentru contorizare nu mai există.
- Este asigurată compatibilitatea cu noi protocoale (pe lângă TCP, UDP și ICMP).
- Contoarele sunt mai mari (64 de biți în loc de 32 de biți).
- Pe lângă *tipurile* ICMP, sunt acceptate și *codurile* ICMP.

Există și alte diferențe, care devin evidente dacă treceți de la *ipfwadm* la *ipchains*. În următoarele secțiuni vom vedea sintaxa folosită pentru *ipchains*.

Crearea și ștergerea înlanțuirilor

Programul *ipchains* lucrează într-o manieră asemănătoare cu programul *ipfwadm*, dar adaugă noi funcții și acceptă protocoale suplimentare. Pentru *ipchains* există trei liste de reguli interne, numite *înlanțuiri* (*chains*), ce pot fi folosite pentru a decide cum este tratat un pachet de intrare sau de ieșire de către gazdă:

- **Înlanțuire de intrare** Reguli pentru gestionarea pachetelor recepționate printr-un adaptor de rețea al gazdei.
- **Înlanțuire de ieșire** Reguli pentru gestionarea pachetelor transmise printr-un adaptor de rețea al gazdei.
- **Înlanțuire de retransmisie** Reguli pentru retransmiterea pachetelor de la un adaptor la altul.

FIGURA 17.1

Pentru fiecare pachet IP primit printr-un adaptor de rețea este verificată fiecare regulă din înlanțuirea de intrare.

Înlanțuire de intrare
Regula 1 nu se potrivește
Regula 2 nu se potrivește
Regula 3 nu se potrivește
Regula 4 se potrivește, pachetului nu i se permite accesul
Regula 5 ignorată
Regula 6 ignorată
Regula 7 ignorată
Regula 8 ignorată
Regula 9 ignorată
Sfârșitul listei

În figura 17.1 puteți vedea o listă de reguli care formează o înlanțuire de intrare. Atunci când un pachet IP este primit de un adaptor de rețea, este comparat cu fiecare regulă din listă.

În această figură, nimic din informațiile conținute de pachetul IP nu se potrivește cu primele

trei reguli. Totuși, este găsită o potrivire pentru a patra regulă, care determină abandonarea pachetului.

Comenzile MASQ și REDIRECT

Pe lângă comenzile `accept`, `deny` și `reject`, programul *ipchains* permite și folosirea comenzilor `masq` și `redirect`. Comanda `masq` vă permite să folosiți caracteristica de mascare IP a nucleului Linux, iar `redirect` vă permite să transmiteți un pachet IP către un soclu de pe gazda locală. Pentru mai multe informații despre folosirea

acestor caracteristici ale programului `ipchains`, vizitați situl Web de bază dedicat programului și analizați exemplele din documentul FAQ sau consultați documentele Linux Masquerade HOW-TO.

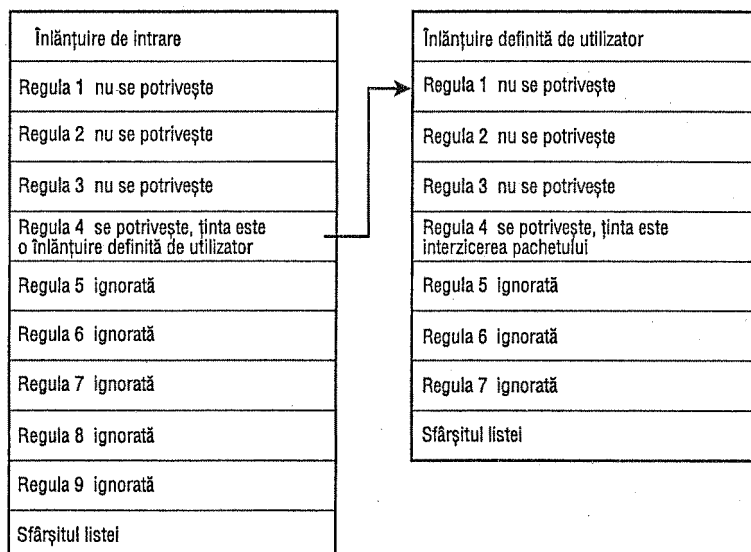
Pe lângă aceste înlanțuiri, puteți folosi comanda `ipchains` și pentru crearea unor înlanțuiri proprii. O înlanțuire definită de utilizator poate fi ținta unei reguli create într-una dintre cele trei înlanțuiri interne. Această posibilitate este utilă pentru crearea unui set de reguli care vor fi folosite pentru testare sau în mai multe înlanțuiri.

Fiecare regulă pe care o adăugați într-o anumită înlanțuire este folosită pentru evaluarea unui pachet IP. Dacă pachetul nu îndeplinește criteriile specificate de prima regulă, este examinată următoarea regulă. Când este găsită o regulă care se potrivește, aceasta specifică ținta pachetului. Ținta poate fi un cuvânt cheie (`accept`, `deny`, `reject` sau `return`) sau numele unei înlanțuiri definite de utilizator. În cel de-al doilea caz, pentru evaluarea pachetului sunt folosite în continuare regulile din înlanțuirea definită de utilizator. Dacă este găsită o regulă potrivită, ținta specificată de regula respectivă este folosită pentru continuarea procesului. Dacă în înlanțuirea definită de utilizator nu este găsită o regulă potrivită, prelucrarea pachetului IP continuă cu înlanțuirea originală, de la următoarea regulă după cea folosită pentru a trimite pachetul către înlanțuirea definită de utilizator.

În figura 17.2 puteți vedea un exemplu de folosire a unei înlanțuiri definite de utilizator.

FIGURA 17.2

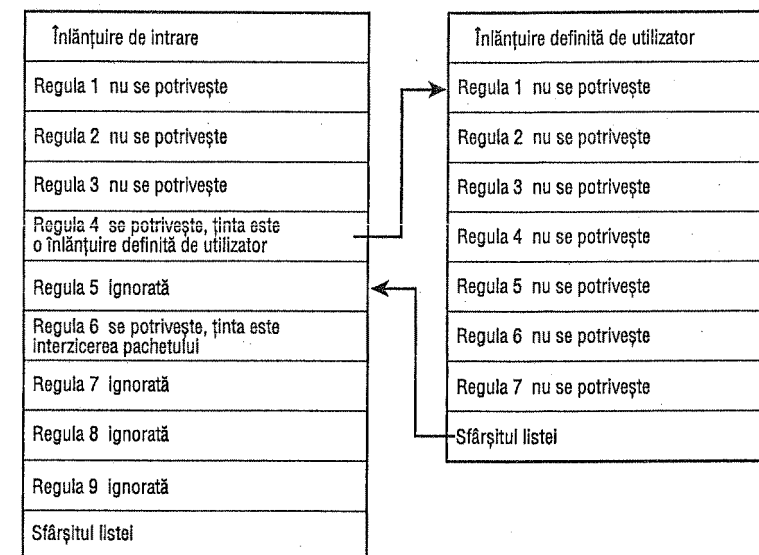
Ținta unei reguli poate fi o înlanțuire definită de utilizator, care conține alte reguli ce trebuie verificate.



În acest caz, este găsită o potrivire a pachetului IP în regula numărul 4 din înlanțuirea de intrare. Ținta acestei reguli nu este `accept`, `deny` sau `reject`, ci o înlanțuire definită de utilizator. Ca urmare, după regula numărul 4, prelucrarea pachetului continuă în înlanțuirea definită de utilizator. În această înlanțuire, primele trei reguli nu conțin criterii care să corespundă pachetului verificat. Totuși, în regula numărul 4 este găsită o potrivire și este interzis accesul pachetului. Atunci când prelucrarea continuă într-o înlanțuire definită de utilizator, nu este obligatoriu să se găsească o regulă corespunzătoare pachetului. În figura 17.3 puteți vedea un alt exemplu de salt la o înlanțuire definită de utilizator.

FIGURA 17.3

Ținta unei reguli poate fi o înlanțuire definită de utilizator, care conține alte reguli ce trebuie verificate.



În acest caz, o înlanțuire definită de utilizator a fost ținta unei reguli din înlanțuirea de intrare. Totuși, în înlanțuirea definită de utilizator nu a fost descoperită nici o regulă potrivită, așa că prelucrarea a fost reluată de la următoarea regulă din înlanțuirea de intrare. În sfârșit, în înlanțuirea de intrare a fost găsită o potrivire în regula numărul 6, care a interzis accesul pachetului.

Dacă pachetul IP trece de toate regulile unei înlanțuiri fără să corespundă nici unui criteriu, soarta îi este decisă de politica prestabilită a înlanțuirii. Din nou, este o idee bună să specificați o politică prestabilită pentru fiecare înlanțuire.

Ținta `return` poate fi folosită pentru a opri prelucrarea regulilor, sărind la sfârșitul înlanțuirii. Dacă folosiți cuvântul cheie `return` într-o înlanțuire predefinită, saltul la sfârșitul înlanțuirii are ca rezultat aplicarea politicii prestabilite a înlanțuirii asupra pachetului. Dacă ținta `return` este întâlnită într-o înlanțuire definită de utilizator, saltul la sfârșitul înlanțuirii determină reluarea prelucrării de la următoarea regulă din înlanțuirea predefinită din care a fost apelată înlanțuirea definită de utilizator.

Gestionarea înlanțuirilor

Sintaxa comenzii `ipchains` pentru crearea înlanțuirilor și gestionarea regulilor dintr-o înlanțuire este destul de simplă:

`ipchains comanda parametri [optiuni]`

Principalele comenzi pentru gestionarea înlanțuirilor sunt următoarele:

- `-N inlantuire` Creează o nouă *inlantuire*.
- `-X inlantuire` Șterge o înlanțuire. Toate regulile din înlanțuire trebuie să fie șterse înainte de a șterge înlanțuirea. Nu puteți șterge înlanțuirile predefinite.
- `-P inlantuire tinta` Stabilește politica pentru o înlanțuire predefinită. Înlanțuirile definite de utilizatori nu au politici prestabilite. Dacă se ajunge la sfârșitul unei înlanțuiri

definite de utilizator fără să fie găsită o regulă potrivită, prelucrarea continuă în înlănțuirea predefinită care a apelat înlănțuirea definită de utilizator.

- **-L inlantuire** Listează regulile dintr-o înlănțuire.
- **-F inlantuire** Șterge toate regulile dintr-o înlănțuire.
- **-Z inlantuire** Reinițializează contoarele de pachete și de octeți pentru toate regulile din înlănțuirea specificată.

Gestionarea regulilor

După cum ați văzut, comenzile de mai sus pot fi folosite pentru manipularea înlănțuirilor. Pentru gestionarea regulilor din fiecare înlănțuire, folosiți programul *ipchains* cu comenzile următoare:

- **-A inlantuire regula** Această comandă adaugă o nouă regulă la o înlănțuire.
- **-I inlantuire numar_de_regula regula** Această comandă inserează o regulă într-o înlănțuire. Regulile sunt numerotate. Specificați poziția în care va fi inserată regula, folosind un *numar_de_regula*.
- **-R inlantuire numar_de_regula regula** Această comandă înlocuiește o regulă existentă (specificată de *numar_de_regula*).
- **-D inlantuire regula sau -D inlantuire numar_de_regula** Șterge o regulă, identificată prin număr sau prin comparare cu parametrul *regula*.

Așa cum ați văzut, comanda *ipchains -D* șterge o regulă. Puteți specifica regula ce urmează să fie ștersă la fel cum ați făcut pentru adăugarea acesteia (*ipchains -A*), înlocuind *-A* cu *-D*. Dacă vreți să folosiți numerele de reguli, executați mai întâi comanda de listare (*ipchains -L*) ca să vedeți regulile, apoi folosiți numărul corespunzător în comanda de ștergere.

Până acum ați văzut cum puteți să creați și să gestionați înlănțuirile sau cum să adăugați și să gestionați regulile. Parametrii (cu litere mici, așa cum veți observa) pe care îi puteți folosi pentru specificarea regulilor sunt următorii:

- **-s sursa** Indică adresa IP a sursei. Aceasta poate fi o gazdă propriu-zisă, o adresă de rețea, un nume de gazdă sau un nume de rețea.
- **-d destinatie** Indică adresa IP a destinației.
- **-p protocol** Indică protocolul. Puteți folosi nume (*tcp*, *udp*, *icmp* sau *all*) sau un număr de protocol (conform definițiilor din */etc/protocols*).
- **-i interfata** Indică interfața de rețea.
- **-j tinta** Sare la o țintă. Acest parametru este folosit pentru indicarea acțiunii executate dacă pachetul IP corespunde regulii. Ținta poate fi o țintă standard (de exemplu, *accept*, *deny*, *reject*) sau numele unei înlănțuiri de reguli definite de utilizator. Dacă nu specificați o țintă, regula nu afectează modul de prelucrare a pachetului.
- **-f** Acest parametru indică faptul că regula este aplicată numai pachetelor fragmentate, după primul fragment.

Atunci când folosiți parametrii *-s* și *-d* pentru specificarea unei adrese, puteți utiliza o adresă IP, un nume de gazdă sau un nume de rețea. Dacă specificați o adresă, puteți specifica și masca de rețea sau numărul de port. În cazul unei adrese IP, puteți specifica

adresa exactă sau un domeniu de adrese. Există două modalități de specificare a unui domeniu de adrese:

- Folosiți simbolul */* pentru specificarea unei măști. Textul *140.176.122.0/255.255.255.0* acoperă orice pachet IP cu adresa între *140.176.122.0* și *140.176.122.255*. Masca *255.255.255.0* arată că sunt luate în considerare numai primii trei octeți ai adresei.
- Folosiți un număr întreg pentru a indica numărul de valori 1 din adresă. Amintiți-vă că valoarea 1 este folosită într-o mască pentru a permite luarea în considerare a poziției unui bit. Ca urmare, textul *140.176.122.0/24* înseamnă același lucru cu *140.176.122.0/255.255.255.0*, deoarece un șir de 24 de valori 1 în binar (*11111111111111111111111100000000*) înseamnă același lucru cu *255.255.255.0*, în notație zecimală cu punct.

Specificarea porturilor în ipchains

Pe lângă folosirea numerelor de porturi cu comenzile *ipchains*, puteți folosi șiruri de caractere pentru multe numere de porturi standard. De exemplu, în loc să folosiți *8080*, puteți folosi *www*. Pentru mai multe informații despre șirurile de caractere specifice, consultați documentul *ipchains FAQ*.

Pentru specificarea unui număr de port, plasați-l după adresă în linia de comandă. Pentru specificarea unui domeniu de porturi, folosiți caracterul *:*. În cazul specificării unui domeniu de porturi, dacă omiteți unul dintre porturi, *ipchains* folosește o valoare prestabilită. Valoarea prestabilită pentru începutul domeniului este 0, iar pentru sfârșitul domeniului de porturi este *65535*. Ca urmare,

1024:1050

specifică toate porturile între 1024 și 1050, în timp ce

:1023

specifică toate porturile între 0 și 1023.

Luând în considerare cele menționate mai sus, haideți să vedem câteva exemple:

ipchains -A input -s 140.176.200.254 -j DENY

În acest exemplu, adăugați (*-A*) la înlănțuirea de intrare o regulă care identifică pachetele cu adresa sursei (*-s*) *140.176.200.254*. Pachetele care corespund acestei reguli sunt trimise către ținta standard *DENY*, ceea ce înseamnă că pachetele sunt abandonate fără să fie returnat sursei un mesaj *ICMP*.

ipchains -A output -p TCP -d 0.0.0.0/0 8080 -j REJECT

În acest exemplu, orice pachet expediat (înlănțuirea de ieșire) folosind protocolul *TCP* (*-p tcp*) către orice adresă destinație (*0.0.0.0/0*) pentru portul *8080* este respins. Ținta *REJECT* înseamnă că va fi returnat sursei un mesaj *ICMP*.

Alte opțiuni pentru comenzi

Pe lângă sintaxa de bază pe care ați examinat-o până acum, *ipchains* pune la dispoziție alte câteva opțiuni pe care le puteți folosi în linia de comandă. Acestea sunt următoarele:

- **-b** Indicator bidirecțional. Această opțiune înseamnă că sunt create două reguli în loc de una singură. A doua regulă este identică cu prima, dar specificațiile pentru sursă și destinație sunt inversate.

- -v Indicatorul „verbose“. Acesta determină comenzile de listare să afișeze informații suplimentare.
- -n Ieșire numerică. Adresele și numerele de porturi sunt afișate în format numeric. În mod prestabilit, afișarea se face sub formă de text (de exemplu, nume de gazde, atunci când sunt cunoscute).
- -l Indicator de înregistrare în jurnal. Această opțiune determină înregistrarea în jurnal a pachetelor de către nucleu.
- -o [*maxsize*] Această opțiune este folosită, în principal de dezvoltatori, pentru a determina copierea pachetelor pe un dispozitiv de utilizator, în vederea examinării ulterioare. Dacă este folosit, parametrul *maxsize* limitează numărul de octeți copiați din fiecare pachet.
- -m *marca* Această opțiune este folosită pentru marcarea pachetelor cu o valoare fără semn pe 32 de biți. Această opțiune este utilă pentru hackeri și nu este folosită prea des.
- -t *andmask xormask* Această opțiune specifică o mască folosită pentru modificarea câmpului TOS (tipul serviciului) din antetul IP. Între câmpul TOS și prima mască se face o operație ȘI pe biți, apoi între rezultat și a doua mască se face o operație XOR pe biți.
- -x Această opțiune determină afișarea valorilor numerice exacte ale contoarelor, în locul valorilor rotunjite.
- -y Această opțiune determină aplicarea regulii asupra pachetelor TCP care au bitul SIN activat și biții ACK și FIN șterși. Opțiunea este folosită în cazul protocolului TCP pentru specificarea pachetelor care solicită o conexiune.

Câteva dintre aceste opțiuni sunt create pentru comoditate, cum ar fi opțiunea -b, care vă permite să creați două reguli în același timp. Opțiunea -y este foarte utilă pentru blocarea încercărilor de creare a conexiunilor TCP. Următorul exemplu poate fi folosit pentru blocarea conexiunilor de la adresa 140.176.200.1:

```
ipchains -A input -p TCP -s 140.176.200.1 -y
```

Un alt truc interesant pe care este bine să îl rețineți este folosirea operatorului de negare (!). De exemplu:

```
ipchains -A output -p TCP ! 140.176.200.1 www
```

Această regulă precizează că toate gazdele, cu excepția celei cu adresa 140.176.200.1, pot transmite pachete *www* prin înlănțuirea de ieșire. Puteți nega și alte părți ale regulii. De exemplu, dacă ați fi plasat operatorul de negare imediat înaintea specificației de port *www*, toate gazdele ar fi putut trimite orice tip de pachete, cu excepția pachetelor *www*.

Folosirea scripturilor pentru salvarea regulilor

Există două comenzi pe care le puteți folosi cu *ipchains* pentru salvarea regulilor într-un fișier și restaurarea acestora. Acestea sunt *ipchains-save* și *ipchains-restore*. De fapt, acestea sunt fișiere script pentru automatizarea funcțiilor respective. De exemplu:

```
ipchains-save> firewallrules
```

Această comandă salvează toate regulile definite în toate înlănțuirile în fișierul *firewallrules*. Dacă folosiți opțiunea -v cu această comandă, este afișat numele fiecărei

înlănțuiri ale cărei reguli sunt salvate. De asemenea, sunt salvate politicile prestabilite pentru înlănțuirile standard înglobate.

Pentru restaurarea regulilor, folosiți celălalt fișier script:

```
ipchains-restore< firewallrules
```

Și în acest caz, opțiunea -v determină afișarea numelui fiecărei înlănțuiri, pe măsură ce sunt restaurate regulile din înlănțuirea respectivă. De asemenea, puteți folosi opțiunea -f. În acest caz, scriptul *restore* vă întreabă la fiecare înlănțuire definită de utilizator dacă vreți să o ștergeți sau să o ignorați.

Alte informații despre programul *ipchains*

Utilitarul *ipchains* este un pas înainte față de utilitarul *ipfwadm*, prin caracteristicile oferite. În acest capitol ați văzut numai sintaxa de bază a comenzilor și modul în care *ipchains* filtrează pachetele IP cu ajutorul listelor de reguli. Pentru a deveni un expert în folosirea sistemului de operare Linux pentru filtrarea pachetelor, ar trebui să citiți mai mult despre acest subiect. După cum vedeți, utilitarul *ipchains* ar putea fi subiectul unei cărți întregi!

Pentru ca lucrurile să fie mai simple, vizitați pagina de bază a utilitarului *ipchains* (www.rustcorp.com/linux/ipchains). În plus, consultați diferitele documente Linux HOWTO, în special „Linux IPCHAINS-HOWTO“, de Paul Russel. Puteți descărca acest document de la adresa: <http://metalab.unc.edu/mdw/HOWTO/IPCHAINS.HOWTO.html>

Nu uitați că *ipchains* este un produs pentru care asistența este asigurată de utilizatori, așa că puteți găsi deseori răspunsuri la întrebări căutând în diferite grupuri de discuții sau abonându-vă la listele poștale referitoare la *ipchains*.

Rezumat

Sistemul de operare Linux conține deja în nucleu codul pentru filtrarea pachetelor. Utilitarele *ipfwadm* și *ipchains* sunt folosite ca interfețe pentru acest sistem de filtrare a pachetelor. Pentru versiunile Linux mai vechi, folosiți utilitarul *ipfwadm*. Pentru versiunile de nucleu mai noi, folosiți utilitarul *ipchains*. Deși ambele utilitare folosesc o sintaxă dificilă pentru începători, avantajele sunt mari. Dacă nu ați instalat deja sistemul de operare Linux pe un calculator din situl dumneavoastră, folosiți o versiune mai nouă, astfel încât să aveți acces la caracteristicile îmbunătățite pe care le oferă *ipchains* față de *ipfwadm*.

Datorită posibilităților de filtrare a pachetelor, un sistem Linux poate fi o suplimentare utilă pentru un firewall. Totuși, nu uitați că pentru construirea unui firewall complet, pe lângă filtrarea pachetelor aveți nevoie și de o aplicație intermediar.

Microsoft Proxy Server

- **Prezentare generală a produsului Microsoft Proxy Server**
- **Instalarea și configurarea produsului Microsoft Proxy Server 2.0**
- **Aspecte legate de configurarea componentelor software client**

Prezentare generală a produsului Microsoft Proxy Server

Atunci când a fost lansată prima versiune a produsului Microsoft Proxy Server, îi lipseau câteva caracteristici, astfel că era incomplet și nu putea fi folosit ca firewall. Versiunea 2.0 a adăugat filtrarea dinamică a pachetelor și alte caracteristici care fac din acest server intermediar o soluție bună pentru multe situații. Poate fi folosit într-o rețea locală mică, în care funcțiile de păstrare în cache pot contribui la reducerea gradului de utilizare a conexiunii la Internet, iar problemele de gestionare a securității sunt minore. De asemenea, poate fi folosit pentru crearea unor matrice de servere intermediar pentru gestionarea serviciilor Internet într-o rețea mare.

Principalele caracteristici pe care le veți găsi în versiunea 2.0 sunt următoarele:

- **Rețele virtuale private (VPN)** – Această opțiune asigură criptarea în rețea pentru clienții de la distanță care trebuie să se conecteze la rețeaua companiei.
- **Păstrarea în cache** – Prin păstrarea în cache a obiectelor solicitate frecvent, serverul intermediar poate contribui la reducerea gradului de utilizare a capacității de transfer a conexiunii la Internet.
- **Intermedierea aplicațiilor** – Aceste servere intermediar contribuie la protejarea clienților care au nevoie de acces la servicii din Internet. Intermediarii împiedică schimburile directe de pachete IP între client și Internet, acționând ca niște mediatori care fac cererile în locul clienților.
- **Traducerea adreselor** – Prin folosirea unuia dintre domeniile rezervate de adrese din rețeaua internă, vă puteți descurca cu un spațiu de adrese mai mic, permițând în același timp serverului intermediar să mascheze adresele interne ale clienților.
- **Filtrarea dinamică a pachetelor** – Puteți activa această opțiune pentru fiecare serviciu intermediar, pentru a îmbunătăți securitatea. Porturile sunt închise și deschise dinamic, în funcție de necesități, așa că administratorul nu este nevoit să creeze un set complex de reguli, implicând un număr mare de porturi.

- **Inversarea gazdelor** – Puteți folosi serverul intermediar pentru a prezenta în Internet pagini Web provenite, de fapt de pe servere Web din rețeaua locală internă.

MS Proxy Server asigură suportul pentru trei servere intermediar:

- WinSock Proxy
- SOCKS Proxy
- Web Proxy

Combinarea dintre filtrarea pachetelor și serviciile de intermediere, împreună cu posibilitățile de înregistrare în jurnale și de avertizare ale acestui pachet, fac din MS Proxy Server un candidat bun pentru rolul de firewall instalat pe un calculator gazdă. Componentele WinSock și SOCKS Proxy implică faptul că sunt disponibile o mulțime de aplicații client/server care vor lucra cu MS Proxy Server. Serverele Web intermediar la nivel de aplicație oferă suport pentru navigarea în Web (HTTP și HTTP-S), transferul fișierelor (FTP) și protocolul Gopher.

Vezi și

➤ Pentru mai multe informații despre SOCKS Proxy, la pagina 241.

În acest capitol veți parcurge procesul de instalare a produsului Proxy Server, apoi veți vedea cum se face configurarea, folosind ca exemplu serviciul Web Proxy.

Instalarea și configurarea produsului Microsoft Proxy Server 2.0

Există câteva condiții ce trebuie îndeplinite înainte de a putea instala MS Proxy Server 2.0 pe o platformă Windows NT Server.

Una dintre cerințe este Internet Information Server 3.0. Dacă instalați sistemul de operare Windows NT 4.0 pornind de la zero, așa cum ar trebui să faceți dacă vreți să creați o platformă sigură ce urmează a fi folosită ca server intermediar, va trebui să instalați și un pachet de servicii (Service Pack) înainte de a instala serverul intermediar. Ca o cerință minimă, instalați Service Pack 3, care modernizează serverul IIS (Internet Information Server) la versiunea 3.0. Totuși, pentru a beneficia de ultimele programe de corectare și de actualizări create pentru NT 4.0, este recomandabilă instalarea ultimului pachet de servicii. Deoarece pachetele de servicii sunt cumulative¹, nu trebuie să instalați decât ultima versiune, nu pe toate cele anterioare.

Unde puteți găsi pachetele de servicii pentru Windows NT

În funcție de locul din care ați obținut CD-urile sursă pentru Windows NT, s-ar putea să aveți un CD cu ultima versiune a pachetului de servicii. Deși Service Pack 3.0 este suficient pentru modernizarea serverului IIS la versiunea 3.0, cel mai bine este să citiți despre acesta și să instalați ultima versiune a pachetului de servicii. Pentru a-l obține, vizitați situl www.microsoft.com/downloads/.

¹ Programele de corectare (patches) sau de modernizare (updates) pot fi cumulative sau incrementale. În cazul modernizărilor incrementale, pentru instalarea ultimei versiuni trebuie să fi instalat succesiv toate versiunile anterioare (n. trad.)

O altă condiție este să aveți o partiție care folosește sistemul de fișiere Windows NT, adică NTFS. O partiție DOS (FAT sau FAT32) nu poate fi folosită pentru stocarea fișierelor de cache pe care le creează Proxy Server. Dacă ați instalat sistemul de operare Windows NT Server într-o partiție FAT, ar trebui să o transformați într-o partiție NTFS, pentru a beneficia de avantajele pe care le oferă aceasta din punctul de vedere al securității. Dacă vreți să folosiți o altă partiție pentru instalarea serverului intermediar, trebuie să transformați partiția respectivă în NTFS înainte de a putea continua.

Transformarea partițiilor FAT în partiții NTFS

Este ușor să transformați o partiție FAT în partiție NTFS. La instalarea sistemului de operare Windows NT, programul de instalare vă cere să formatați ca partiție NTFS discul pe care îl folosiți pentru instalare. Dacă instalați sistemul de operare Windows NT Server pe o platformă ce urmează să fie folosită ca server intermediar, este logică transformarea partiției în timpul instalării. Totuși, dacă ați instalat deja sistemul de operare și aveți o partiție FAT sau FAT32, puteți folosi comanda CONVERT pentru a schimba sistemul de fișiere în NTFS:

```
C:\> CONVERT D: /FS:NTFS
```

Dacă folosiți această comandă pentru unitatea de disc care conține sistemul de operare, trebuie să reîncărcați sistemul pentru ca modificarea să aibă efect.

Ca întotdeauna, înainte de a face orice modificare importantă într-un sistem, nu uitați să faceți o copie de siguranță completă a discului pe care vreți să îl transformați! Niciodată nu puteți fi sigur că nu se va întâmpla ceva nedorit. De exemplu, în timpul transformării discului poate avea loc o cădere de tensiune care să cauzeze blocarea sistemului, ceea ce duce la pierderea datelor.

Înainte de instalare trebuie să verificați și îndeplinirea următoarelor condiții:

- Folosiți un calculator Windows NT Server instalat ca server independent, care nu îndeplinește funcția de controller de domeniu. În mod prestabilit, un controller de domeniu stochează informații sensibile, cum ar fi o copie a bazei de date SAM în care sunt păstrate conturile utilizatorilor și relațiile de încredere ale domeniului. Desigur, nu doriți ca informații de acest tip să se afle pe un server intermediar.
- Pentru a folosi posibilitățile de filtrare a pachetelor oferite de versiunea 2.0, folosiți un calculator gazdă pe care sunt instalate două interfețe de rețea – una conectată la rețeaua locală internă și una conectată la Internet. Folosind două interfețe de rețea și, ca urmare, izolând complet rețeaua internă de o conexiune IP directă la Internet, transformați serverul intermediar într-un punct obligatoriu de trecere pentru tot traficul de rețea. În acest fel, un utilizator descărcăreț nu își poate reconfigura stația de lucru astfel încât să ocolească serverul intermediar și să comunice direct cu ruterul extern.

Rularea programului de instalare

Atunci când executați programul de instalare pentru MS Proxy Server, primele casete de dialog sunt cele standard pe care le vedeți de obicei la instalarea aplicațiilor sub Windows NT Server – Software License și Copyright. În continuare, sunteți invitat să introduceți cheia de CD pentru software. Apoi, programul de instalare începe să vă pună întrebări despre instalarea componentelor software ale serverului intermediar.

Instalarea serverului intermediar

FIGURA 18.1

Folosiți caseta de dialog Installation Options pentru a schimba dosarul în care se face instalarea sau pentru a selecta aplicațiile ce vor fi instalate.

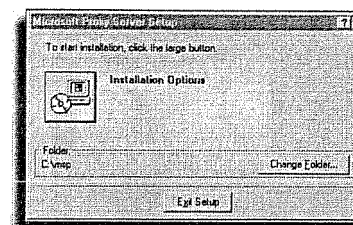


FIGURA 18.2

Puteți opta pentru instalarea documentației și a aplicației Administration Tool împreună cu aplicația Proxy Server.

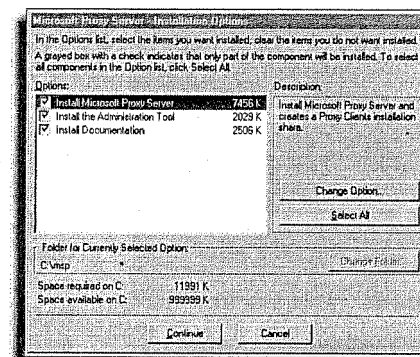
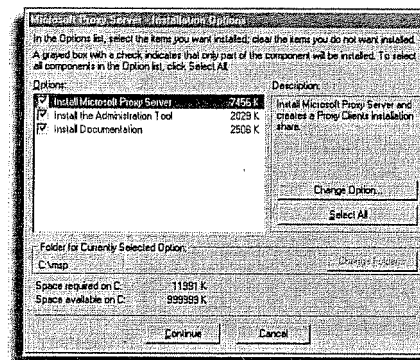


FIGURA 18.3

Selectați partiția (unitatea de disc) ce va fi folosită pentru fișierele de cache și stabiliți dimensiunea inițială a zonei în care vor fi stocate aceste fișiere.



1. Caseta de dialog Installation Options (figura 18.1) vă permite să schimbați unitatea de disc și dosarul în care va fi instalat produsul Proxy Server. Pentru a face acest lucru, executați clic pe butonul Change Folder.

2. Butonul Installation Options (butonul mare) din această casetă de dialog poate fi folosit pentru a selecta componentele Proxy Server pe care vreți să le instalați, așa cum puteți vedea în figura 18.2. Pentru prima instalare, selectați toate cele trei componente.

3. Următoarea casetă de dialog vă invită să selectați unitatea de disc pe care vor fi păstrate fișierele de cache (figura 18.3). Nu uitați că acest disc trebuie să fie formatat folosind sistemul de fișiere NTFS. De asemenea, puteți folosi această casetă de dialog pentru a stabili dimensiunea cache-ului.

La prima instalare păstrați valoarea prestabilită.

4. Următoarea casetă de dialog (figura 18.4) vă permite să introduceți unul sau mai multe domenii de adrese folosite în rețeaua locală internă. Dacă folosiți butonul Construct Table din această casetă de dialog, programul de instalare vă permite să selectați domenii de adrese pe care le găsește în tabelul de rutare al serverului (figura 18.5). Selectarea unui domeniu de adrese privat vă pune la dispoziție un spațiu mare de adrese, care nu sunt folosite direct în Internet. Pentru asigurarea acestei funcții, Proxy Server folosește translatarea adreselor de rețea (NAT). Dacă folosiți opțiunea de

FIGURA 18.4

Pentru a defini spațiul de adrese al rețelei locale interne, introduceți adresele de început și de sfârșit ale domeniului și executați clic pe butonul Add.

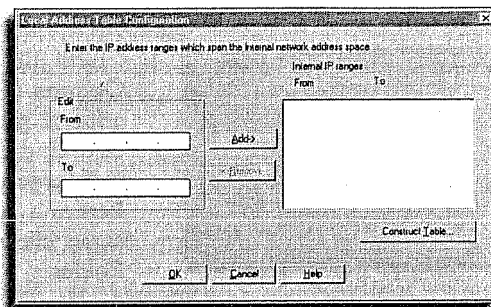


FIGURA 18.5

Puteți să adăugați domenii de adrese din tabelul de rutare local sau să selectați un domeniu de adrese particular.

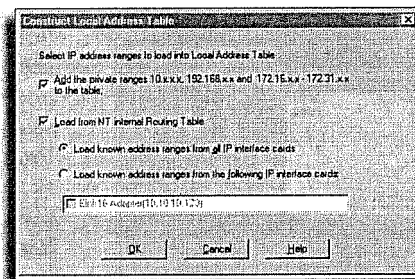
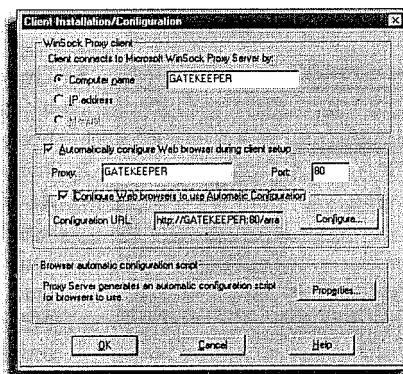


FIGURA 18.6

Configurați informațiile de instalare a clienților folosind această casetă de dialog.



butonul Properties, vi se permite să specificați domenii sau gazde pentru care nu este asigurată intermedierea (vezi figura 18.7). Această opțiune poate fi folosită nu numai pentru a permite clienților locali accesul direct la serviciile din LAN, ci și pentru a utiliza serverul Proxy pentru toate serviciile legate de Internet.

- Următoarea casetă de dialog, Access Control (figura 18.8), vă permite să activați controlul accesului pentru clienți. Puteți activa controlul accesului pentru WinSock, Web Proxy sau pentru ambele servicii.
- În final, sunt copiate câteva fișiere, apare o casetă de mesaje care vă informează că puteți configura filtrarea pachetelor folosind instrumentul de administrare, iar ultima casetă de dialog vă informează că MS Proxy Server a fost instalat cu succes.

încărcare a tabelului de rutare, programul de instalare vă invită să editați domeniile de adrese care par a proveni din afara rețelei locale. Sursa acestora ar putea pot fi conexiunile curente la Internet.

- Următoarea casetă de dialog vă permite să configurați unele informații referitoare la clienți. Clienții se pot conecta la server după nume sau după adresa IP. Puteți să decideți dacă clienții se vor conecta la portul 80 pentru a intra în legătură cu serverul intermediar sau să specificați o adresă URL a unui fișier de configurare pentru încărcarea unor configurații mai complexe ale clienților.

Dacă este selectată caseta Configure Web browsers, puteți să apăsați butonul Configure, apoi să introduceți o adresă URL care va fi folosită de clienți pentru autoconfigurarea informațiilor pentru Proxy Server. Dacă executați clic pe

FIGURA 18.7

Pentru configurarea automată a clienților, puteți selecta servere sau domenii locale care nu vor folosi serverul intermediar.

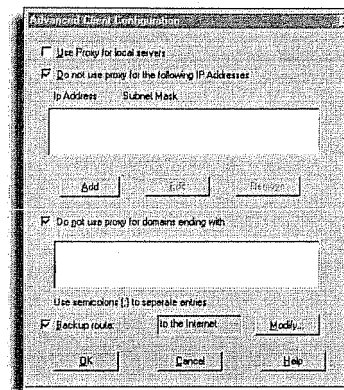
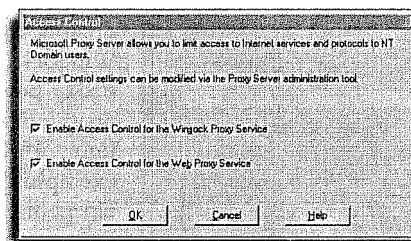


FIGURA 18.8

Activați controlul accesului folosind această casetă de dialog.



Folosirea programului Internet Service Manager

După ce ați instalat programul Proxy Server, veți găsi în dosarul Programs un nou dosar, numit Microsoft Proxy Server. Aplicația Internet Service Manager din acest dosar este folosită pentru gestionarea serviciilor oferite de Proxy Server. Pentru lansarea, oprirea sau întreruperea unui serviciu, evidențiați-l, apoi selectați una dintre comenzile Start, Stop sau Pause din meniul Properties.

Pentru configurarea unui serviciu, puteți să îl evidențiați, apoi să selectați opțiunea Service Properties din meniul Properties, sau puteți să executați clic cu butonul din dreapta pe serviciu, apoi să selectați opțiunea Service Properties din submeniul care apare.

Proprietăți pentru filtrarea pachetelor

Puteți configura filtrarea pachetelor, statică sau dinamică, folosind pagina Properties pentru serviciile SOCKS, WinSock sau Web Proxy din utilitarul Microsoft Internet Service Manager. În exemplul următor veți vedea procesul parcurs pentru serviciul WinSock.

Configurarea filtrării pachetelor

- Executați clic pe Start, Programs, Microsoft Proxy Server, Internet Service Manager.
- Fereastra principală a utilitarului (figura 18.9) afișează serviciile aflate în execuție.

FIGURA 18.9

Utilitarul Internet Service Manager afișează serviciile de intermediere aflate în execuție.

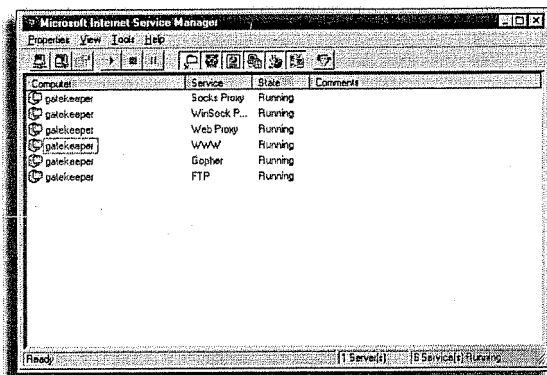


FIGURA 18.10

Pentru a activa filtrarea pachetelor, selectați butonul Security din foaia de proprietăți a serviciului.

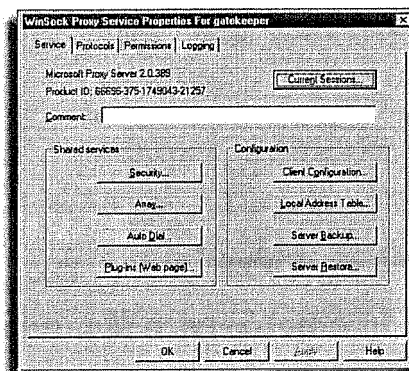
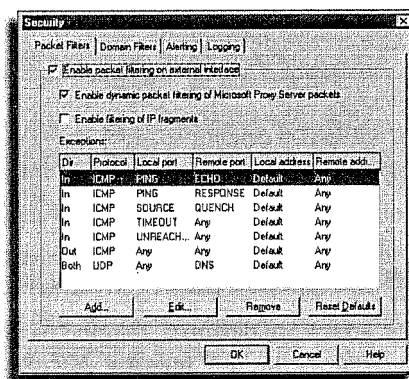


FIGURA 18.11

Puteți activa filtrarea pachetelor folosind această casetă de dialog.



trarea dinamică a pachetelor sau să ștergeți și să modificați regulile din configurația prestabilită. De exemplu, folosiți butonul Add ca să adăugați o regulă pentru un serviciu specializat. Casetă de dialog care apare (prezentată în figura 18.12) vă permite să configurați o regulă de filtrare a pachetelor pe baza protocolului, a direcției (trafic de intrare sau de ieșire) și a porturilor sursă și destinație.

Executați clic cu butonul din dreapta pe SOCKS Proxy, WinSock Proxy sau Web Proxy pentru a afișa foile de proprietăți ale serviciilor. În figura 18.10, puteți vedea un exemplu de foaie de proprietăți pentru serviciul WinSock Proxy.

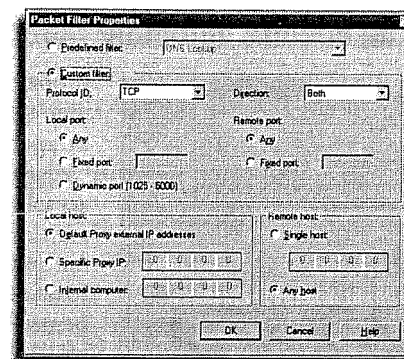
3. Executați clic pe butonul Security ca să afișați foile de proprietăți Security, dintre care prima este numită Packet Filters (vezi figura 18.11).

Pentru a activa filtrarea pachetelor, selectați ambele casete de validare de pe această pagină: Enable Packet Filtering On External Interface și Enable Dynamic Packet Filtering of Microsoft Proxy Server Packets.

4. În rubrica Exceptions puteți să adăugați reguli pentru crearea unor excepții la fil-

FIGURA 18.12

Puteți configura porturi statice și dinamice folosind această casetă de dialog.



un port și nu pot fi utilizate porturile selectate dinamic. După ce terminați de adăugat o regulă, executați clic pe butonul OK. Folosiți în continuare butonul Add pentru adăugarea altor reguli.

6. După ce terminați, executați clic pe butonul OK de pe pagina Packet Filter Properties ca să ieșiți.

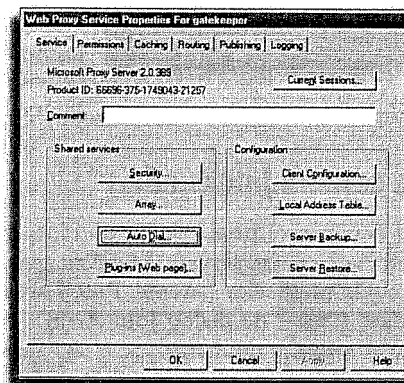
Posibilitatea de stabilire a unor reguli foarte explicite pentru un filtru de pachete, în funcție de serviciu, vă oferă o mare flexibilitate. Puteți să optați pentru filtrarea dinamică a pachetelor, să rămâneți la reguli statice sau să le folosiți pe amândouă.

Filtrarea dinamică a pachetelor în MS Proxy Server începe atunci când un client face o cerere pentru un serviciu prin WinSock Proxy. Clientul intermediar se conectează la MS Proxy Server, care autentifică utilizatorul, apoi creează un soclu folosind un număr de port aleatoriu. Gestionarul filtrului de pachete primește acest număr de port, apoi permite pachetelor primite sau transmise să treacă prin filtru pentru această sesiune și aplicație. Atunci când clientul termină conexiunea, portul este închis și nu poate fi folosit de o altă aplicație.

Proprietățile serviciului Web Proxy

FIGURA 18.13

Pagina de proprietăți pentru serviciul Web Proxy vă permite să controlați accesul și aspectele de gestionare.



5. Folosind această casetă de dialog, puteți configura reguli foarte precise pentru filtrarea pachetelor. Puteți configura un port fix sau dinamic pentru sursă și destinație și un număr de gazde din Internet. Folosiți această casetă de dialog pentru configurarea unor conexiuni speciale atunci când trebuie să specificați

În figura 18.13 puteți vedea pagina de proprietăți a serviciului Web Proxy. Și în acest caz puteți folosi butonul Security de pe pagina de proprietăți Service pentru a activa filtrarea pachetelor pe serverul intermediar, așa cum am arătat pentru serverul WinSock Proxy în secțiunea anterioară.

Există câteva aspecte interesante pe care le puteți controla folosind foile de proprietăți și, în această secțiune, veți vedea câteva dintre acestea, folosind ca exemplu aplicația Web Proxy. În grupul Shared Services se află patru butoane folosite pentru gestionarea serviciilor oferite de serverul intermediar.

Configurarea proprietății de apelare automată (Auto Dial)

FIGURA 18.14

Selecționați orele și zilele în care este activă apelarea automată.

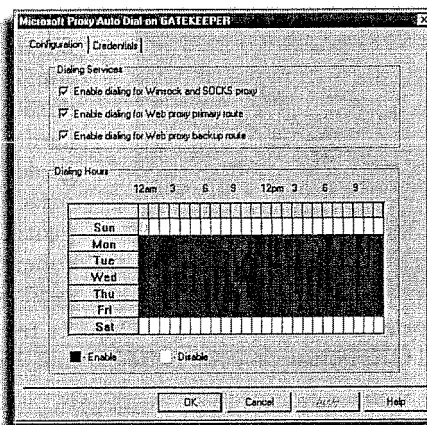
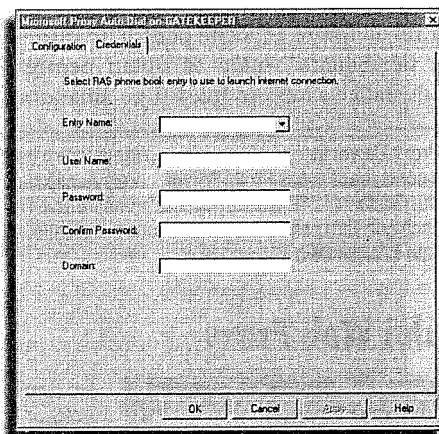


FIGURA 18.15

Puteți să selecționați un cont existent sau să introduceți informațiile necesare pentru unul nou.



Proprietatea Auto Dial permite serverului intermediar să apeleze automat o conexiune Internet atunci când aceasta este asociată cu un serviciu. Executați clic pe butonul Auto Dial de pe foaia de proprietăți Service pentru a afișa foaia de proprietăți pentru Auto Dial (vezi figura 18.14).

În această casetă de dialog puteți folosi mouse-ul pentru a selecta, în intervale de câte o oră, zilele și orele în care este activă proprietatea Auto Dial. Opțiunile Dialing Services din partea de sus a acestei casete de dialog vă permit să activați apelarea automată pentru serviciile SOCKS, WinSock și Web Proxy. Dacă selecționați eticheta din partea de sus a casetei de dialog pentru a afișa foaia de proprietăți Credentials, puteți să selecționați un cont folosit pentru conexiune și să introduceți informațiile de autentificare necesare acestui cont (vezi figura 18.15).

Intrarea într-o matrice de servere intermediar

Butonul Array din grupul Shared Services vă permite să intrați într-o matrice de servere intermediar pentru a schimba informații cu alte servere. După ce apăsați butonul Array, o casetă de dialog afișează configurațiile matricelor curente. Puteți apoi să folosiți butonul Add ca să intrați într-o altă matrice. Casetă de dialog Join Array vă cere să introduceți numele unui alt calculator. Dacă este creată o nouă matrice, o altă casetă de dialog vă cere să introduceți numele matricei.

Folosirea mai multor servere MS Proxy care conlucrează într-o matrice vă poate ajuta să distribuiți încărcarea, dacă aveți un număr mare de utilizatori care folosesc serviciile intermediare. Serverele aflate în aceeași matrice folosesc comunicații peer-to-peer pentru

schimburile de informații. De asemenea, o matrice asigură și toleranța la defectări, deoarece căderea unui singur server intermediar nu împiedică accesul la Internet. De asemenea, este posibilă executarea unor funcții de gestionare pe mai multe servere simultan, dacă acestea sunt membre ale unei matrice.

Componente suplimentare produse de terți

Butonul Plugs din grupul Shared Services de pe pagina de proprietăți Services vă permite să descărcați componente produse de alți dezvoltatori pentru serverul Microsoft Proxy. Folosirea acestei opțiuni vă permite să specificați o adresă URL a unei pagini Web cu componente suplimentare (plug-ins). De pe pagina respectivă puteți alege componenta suplimentară ce urmează să fie instalată.

Gestionarea configurației pe pagina de proprietăți Service

În partea dreaptă a paginii de proprietăți Service pentru serviciul Web Proxy se află un grup de butoane, sub eticheta Configuration. Aceste butoane pot fi folosite pentru modificarea informațiilor de configurare despre server și clienți, similar cu cele din casetele de dialog afișate în timpul instalării produsului.

De exemplu, butonul Client Configuration afișează caseta de dialog prezentată în figura 18.6, mai devreme în acest capitol. Puteți folosi această casetă de dialog ca să schimbați modul în care clienții se conectează la serverul intermediar (prin nume sau prin adresa IP) și să specificați informațiile de configurare a clienților, cum ar fi adresele la care are acces Proxy Server.

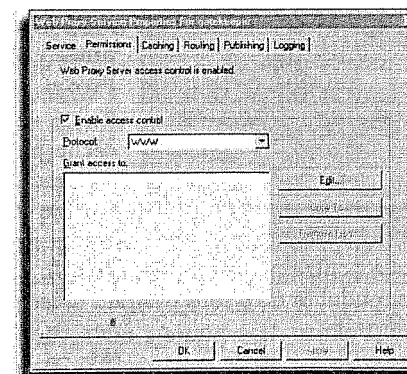
Butonul Local Address Table afișează o altă casetă de dialog pe care ați văzut-o în timpul instalării, prezentată în figura 18.4. Aici puteți specifica domeniile de adrese care vor fi folosite de calculatoarele din rețeaua internă protejată.

Butonul Server Backup vă permite să selecționați un director folosit pentru salvarea informațiilor de configurare a serverului Proxy. Butonul Server Restore vă permite să executați o restaurare parțială sau completă a informațiilor de configurare din fișierul salvat anterior.

Gestionarea permisiunilor pentru serviciile Web Proxy

FIGURA 18.16

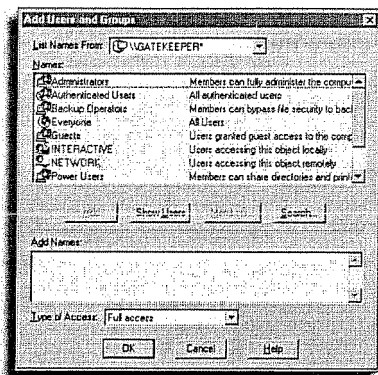
Pagina de proprietăți Permissions poate fi folosită pentru a controla accesul la serviciile Web Proxy.



Eticheta Permissions afișează pagina de proprietăți Permissions pentru serverul Web Proxy. În figura 18.16 puteți vedea că această pagină vă permite, prin butonul Edit, să selecționați un serviciu (folosind câmpul Protocol) și să asociați utilizatori sau grupuri cu permisiuni pentru folosirea serviciului.

FIGURA 18.17

Selecția utilizatorilor sau grupurilor de utilizatori cărora vreți să le permiteți accesul la Web Proxy.



Show Users pentru a selecta conturi individuale de utilizatori.

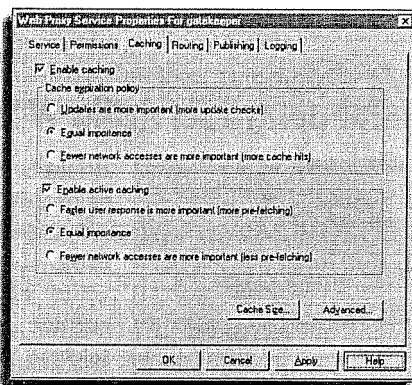
Fii foarte atent atunci când permiteți accesul la o aplicație intermediar unui întreg grup de utilizatori. Dacă numai o parte a grupului trebuie să aibă acces sau dacă trebuie să acordați dreptul de acces mai multor utilizatori din grupuri diferite, probabil că este mai bine să creați un nou grup de utilizatori și să faceți acești utilizatori membri ai noului grup.

Gestionarea proprietăților de cache ale serviciului

Un server intermediar asigură un serviciu de securitate atunci când maschează identitatea gazdelor interne care trebuie să aibă acces la un serviciu Internet. De asemenea, un server intermediar poate fi folosit pentru a îmbunătăți performanțele acestor servicii, păstrând copii ale obiectelor solicitate frecvent într-un cache local. Cererile ulterioare pentru aceste obiecte pot fi satisfăcute din cache, ceea ce economisește lărgimea de bandă folosită pentru conexiunea Internet.

FIGURA 18.18

Pagina de proprietăți Caching poate fi folosită pentru a stabili cât timp sunt păstrate obiectele în cache.



puteți să selectați o politică generală pentru păstrarea obiectelor în cache sau să folosiți butonul Advanced pentru a stabili modul în care sunt păstrate obiectele în cache.

În grupul Cache Expiration Policy (Politica de expirare a cache-ului), puteți selecta una dintre cele trei politici generale:

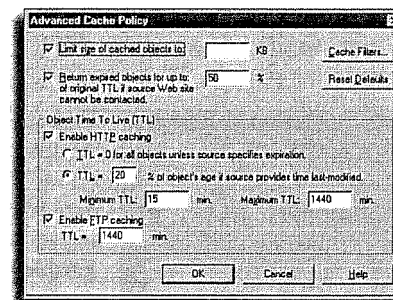
Câmpul Protocol vă permite să selectați serviciile FTP Read, Gopher, Secure și WWW. Atunci când executați clic pe butonul Edit, apare o casetă de dialog care afișează permisiunile curente pentru serviciu, dacă există. Puteți apoi să folosiți butonul Add pentru afișarea unei casete de dialog standard Windows NT Add Users and Groups (figura 18.17). Aici puteți să selectați grupuri de utilizatori sau să folosiți butonul

- **Actualizările sunt mai importante** (mai multe verificări pentru actualizări) Această opțiune cere serverului intermediar să descarce mai frecvent obiectele.
- **Reducerea operațiilor de acces la rețea este mai importantă** (mai multe reușite ale cache-ului) Această opțiune este folosită pentru a îmbunătăți timpul de răspuns la cererile utilizatorilor. Cache-ul este folosit mai mult pentru satisfacerea cererilor.
- **Importanță egală** Această opțiune cere serverului să opereze într-o manieră care echilibrează celelalte două opțiuni.

În cele mai multe cazuri, probabil că ar trebui să folosiți mai întâi opțiunea Equal Importance (Importanță egală), apoi, în funcție de informațiile primite de la utilizatori, să alegeți una dintre celelalte două opțiuni. Dacă datele pe care le primesc utilizatorii se schimbă rareori, a treia opțiune reduce gradul de utilizare a lărgimii de bandă a conexiunii Internet. În această categorie intră obiecte precum documentația producătorilor, deși utilizatorii care obțin date financiare probabil că nu vor agreea această opțiune, deoarece datele de acest tip se modifică mult mai frecvent.

FIGURA 18.19

Caseta de dialog Advanced Cache Policy permite controlul mai precis al modului în care sunt păstrate obiectele în cache.



Butonul Advanced vă permite să specificați dimensiunea obiectelor păstrate în cache și să controlați mai precis durata de viață a acestora (TTL – Time-To-Live) – timpul cât sunt păstrate în cache, înainte de a fi considerate invalide. Figura 18.19 prezintă caseta de dialog Advanced Cache Policy.

Pentru a limita dimensiunea obiectelor stocate în cache, selectați caseta de validare aflată în partea de sus a casetei de dialog (Limit size of cached objects to:) și introduceți o valoare (în KB) pentru dimensiunea maximă. A doua casetă de validare poate fi folosită pentru a cere serverului Proxy să păstreze o perioadă mai lungă în cache o înregistrare expirată, dacă nu mai poate lua legătura cu situl Web original.

Deși, de obicei, serverul Proxy stabilește ce obiecte sunt păstrate în cache, în funcție de utilizare, puteți cere ca anumite adrese URL să fie incluse întotdeauna în cache, folosind butonul Cache Filters (Filtre de cache). Acesta afișează o casetă de dialog pe care o puteți folosi pentru a introduce, una câte una, adresele URL care vă interesează.

În grupul Object Time To Live (TTL) se află câteva butoane care vă permit să controlați durata de păstrare în cache a obiectelor pentru serviciile HTTP și FTP. În primul rând, trebuie să activați păstrarea în cache pentru HTTP și FTP, selectând casetele de validare corespunzătoare.

Sub eticheta Enable HTTP Caching (Activează păstrarea în cache pentru HTTP), puteți preciza că valoarea TTL este 0 dacă sursa datelor nu specifică o durată de expirare, sau puteți selecta al doilea buton radio dacă doriți ca durata de viață a obiectului să fie un procent din vârsta acestuia, în funcție de momentul în care a fost modificat ultima dată. Și această informație trebuie să fie furnizată de serverul gazdă. Ultimele două câmpuri din grupul HTTP vă permit să specificați intervalele de timp minim și maxim (în minute) în care obiectele se pot afla în cache fără să fie considerate expirate.

Rutarea în matricele de servere intermediar

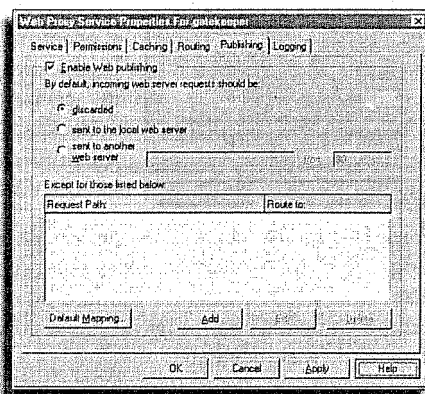
Pagina de proprietăți Routing (Rutare) vă permite să gestionați modul în care sunt tratate cererile clienților într-o matrice de servere intermediar. Puteți preciza că cererile sunt trimise direct în Internet, către un server intermediar de pe un nivel superior sau către o altă matrice de servere. Dacă aveți mai multe servere intermediar grupate într-o matrice, puteți echilibra performanțele configurând unele servere pentru un anumit serviciu și celelalte servere pentru alte servicii. Configurând modul în care sunt rutate cererile clienților, puteți direcționa rapid cererile către serverul intermediar care le poate rezolva. Dacă nu aveți o matrice de servere, nu este nevoie să folosiți această pagină de proprietăți.

Folosirea paginii de proprietăți Publishing

Microsoft Proxy Server poate permite clienților din rețeaua internă să publice pagini Web prin serverul intermediar. În acest fel, clienții interni sunt protejați împotriva eventualelor hackeri din exteriorul rețelei locale, dar își pot manifesta prezența în Web. Serverul intermediar acționează ca interfață front-end pentru toate serverele Web pe care le aveți în rețea.

FIGURA 18.20

Puteți folosi această pagină de proprietăți pentru a permite clienților să publice pagini Web prin serverul intermediar.



Pagina de proprietăți Publishing (Publicare) a serviciului Web Proxy este prezentată în figura 18.20. Selectați caseta de validare Enable Web Publishing dacă vreți să permiteți clienților să folosească acest serviciu. În partea de sus a acestei pagini se află trei butoate radio care stabilesc ce se face cu cererile primite. În jumătatea de jos a paginii puteți specifica excepțiile de

la aceste reguli. De exemplu, puteți preciza că toate cererile HTTP sunt respinse (sau ignorate), apoi să specificați câteva excepții, pentru serverele Web cărora le permiteți accesul prin firewall. De asemenea, puteți direcționa cererea către un server Web local (serviciul IIS rulat pe nodul local) sau către un alt server Web. Și aceste opțiuni sunt modificate de excepțiile specificate în fereastra aflată mai jos.

Pentru specificarea unei excepții, folosiți butonul Add. Acesta afișează caseta de dialog Mapping, unde puteți introduce două informații pentru crearea unei mapări:

- **Calea de acces solicitată** Adresa URL a serverului Web către care este trimisă cererea.
- **Adresa URL** Adresa URL a serverului Web care va răspunde cererii.

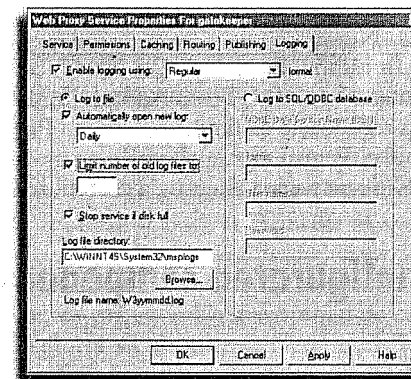
Prin folosirea mapării, este ușor să trimiteți cererile primite către o altă adresă URL, ceea ce vă ajută să ascundeți de lumea exterioară informațiile despre rețeaua internă.

Stabilirea alarmelor în timp real și opțiunile de înregistrare în jurnal

Înregistrarea în jurnal și alarmele sunt unele dintre cele mai importante funcții ale unui firewall. Indiferent de modul în care este creată politica de securitate a rețelei dumneavoastră, niciodată nu puteți fi sigur că prin firewall nu trec informații pe care ar trebui să le studiați. Fișierele jurnal și alarmele vă pot ajuta să răspundeți rapid la evenimentele suspecte și vă furnizează datele necesare pentru identificarea atacatorului.

FIGURA 18.21

Pagina de proprietăți Logging poate fi folosită pentru configurarea fișierelor jurnal sau pentru trimiterea datelor de consemnare către o bază de date compatibilă ODBC.



În figura 18.21 este prezentată pagina de proprietăți Logging pentru serviciul Web Proxy.

Pentru activarea înregistrării în jurnal, selectați caseta de validare Enable Logging Using, apoi folosiți meniul derulant ca să selectați unul dintre formatele Regular sau Verbose. Formatul Verbose determină înregistrarea în jurnal a mai multor informații, în timp ce

formatul Regular determină înregistrarea unui subset de informații disponibile.

Există două metode de înregistrare a evenimentelor: în fișiere jurnal sau într-o bază de date. Pentru transmiterea evenimentelor ce trebuie înregistrate către o bază de date compatibilă ODBC, selectați butonul radio Log to SQL/ODBC Database și completați informațiile de autentificare și de identificare a sursei. Atunci când folosiți această opțiune, ar trebui să vă consultați cu administratorul de baze de date, astfel încât să poată fi create tabelele de care aveți nevoie.

Dacă selectați butonul radio Log to File, puteți specifica și alți parametri de gestionare:

- **Deschide automat un nou jurnal** Dacă selectați această opțiune, puteți să cereți crearea unui nou jurnal în fiecare zi, săptămână sau lună.
- **Limitarea numărului de fișiere jurnal vechi** Atunci când este creat un nou fișier jurnal, fișierul jurnal existent este redenumit, astfel încât să fie păstrat în vederea arhivării. Folosiți această opțiune pentru a limita numărul de fișiere jurnal păstrate.
- **Oprește serviciul dacă discul este plin** Folosiți această opțiune dacă vreți ca serverul intermediar să oprească serviciul de înregistrare în jurnal atunci când pe discul unde sunt stocate fișierele jurnal nu mai este spațiu liber.

În partea de jos a paginii puteți selecta locul unde sunt stocate fișierele jurnal. Prin convenție, numele fișierului este serviciul, plus data în format yymmdd. Ideal ar fi să păstrați fișierele jurnal atât timp cât aveți destul spațiu la dispoziție. Dacă securitatea este aspectul cel mai important în rețeaua dumneavoastră, ar trebui să copiați periodic fișierele jurnal arhivate produse de Proxy Server într-o altă locație, astfel încât să poată fi salvate off-line. Pot trece săptămâni sau luni de la o intruziune în rețea înainte ca pagubele să

devină evidente. Cauza poate fi un program de tip cal troian. Posibilitatea de a vedea cum s-a pătruns în rețea sau de ce configurația dumneavoastră nu a împiedicat pătrunderea vă poate ajuta să vă pregătiți pentru viitor.

Pentru configurarea unei alarme prin e-mail, folosiți butonul Security din grupul Shared Services de pe pagina Service pentru configurarea programului Internet Service Manager. Aici puteți selecta tipul evenimentului care va genera o alarmă. Selectați caseta de validare Send SMTP Mail. Puteți apoi să configurați contul e-mail care va primi mesajele.

În caseta de dialog Security selectați pagina Alerting, apoi executați clic pe butonul Configure Mail. Apare caseta de dialog Configure Mail Alerting, care vă cere să introduceți numele serverului de poștă electronică. Pentru securitate, asigurați-vă că ați specificat un server intern de poștă electronică. Nu ar trebui să aveți încredere într-un server extern pentru raportarea evenimentelor. În câmpul Send Mail To, introduceți adresa e-mail către care vor fi trimise mesajele de alarmare. În câmpul From Address introduceți o adresă validă de poștă electronică pe care o veți recunoaște ca fiind a sistemului Proxy Server. Executați clic pe butonul OK când ați terminat. Pentru a testa alarmele prin e-mail, executați clic pe butonul Test, apoi pe butonul OK de pe pagina Alerting a casetei de dialog Security.

Aspecte legate de configurarea componentelor software client

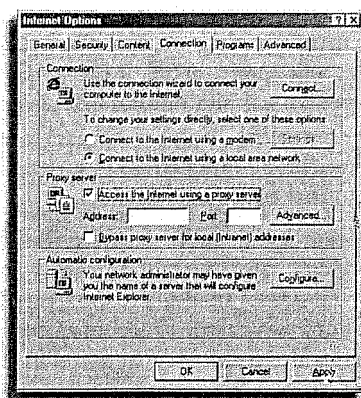
Cele mai multe produse software pentru Internet rulate pe platforme Windows știu să comunice cu un server Proxy. Netscape și Microsoft Internet Explorer au opțiuni care le permit să folosească servere intermediar pentru serviciile Internet. De exemplu, dacă doriți să specificați un server intermediar pentru Internet Explorer (IE), obțineți mai întâi numele sau adresele și porturile folosite pentru serverele intermediar de la administratorul de rețea, apoi parcurgeți următoarele etape:

Utilizarea serverelor intermediar pentru serviciile Internet

1. În Internet Explorer, selectați comanda Internet Options din meniul View. Sunt afișate foile de proprietăți Internet Options.

FIGURA 18.22

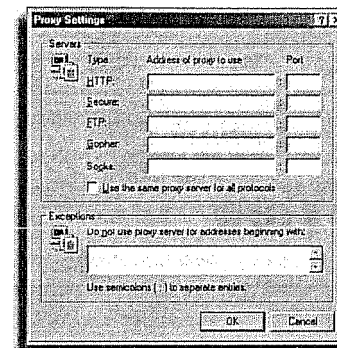
Folosiți pagina de proprietăți Connection ca să configurați clientul pentru utilizarea unui server intermediar.



2. Selectați foaia de proprietăți Connection, executând clic pe eticheta Connection din partea de sus a paginii (vezi figura 18.22). Selectați caseta de validare Access the Internet Using a Proxy Server. Dacă pentru toate serviciile Internet este folosit un singur server intermediar, introduceți aici adresa și numărul de port folosite de acesta.

FIGURA 18.23

În această casetă de dialog puteți specifica un server intermediar diferit pentru fiecare serviciu pe care îl va folosi clientul.



3. Dacă vreți să specificați diferite servere sau porturi pentru fiecare serviciu, executați clic pe butonul Advanced. Acesta afișează caseta de dialog Proxy Settings (vezi figura 18.23).

De asemenea, puteți specifica excepții care nu folosesc serverul intermediar. Acestea ar putea fi, de exemplu, servere Web interne, care nu fac parte din Internet. Clienții din rețeaua locală au acces

direct la acestea, fără să rezulte probleme de securitate, deoarece nu trebuie să treacă prin firewall.

4. După ce terminați de configurat informațiile referitoare la serverul intermediar, puteți executa clic pe butonul OK pentru a aplica modificările făcute.

Într-o rețea mare, ar fi obositor dacă ar fi nevoie să introduceți o mulțime de informații referitoare la serverul intermediar pentru fiecare client. De obicei, puteți scrie un script de configurare pentru clienți, apoi să-i lăsați pe aceștia să specifice adresa URL a paginii la care trebuie să aibă acces pentru rularea scriptului de configurare. În figura 18.22, puteți vedea că Internet Explorer vă permite să faceți acest lucru folosind butonul Configure, aflat în partea de jos a foii de proprietăți, sub eticheta Automatic Configuration.

Posibilitățile de configurare automată diferă de la un browser la altul, dar, în general, vă permit să specificați nu numai datele de configurare pentru serverul intermediar, ci și alți parametri, cum ar fi pagina de bază prestabilită a utilizatorului. Verificați documentația browserului pe care îl aveți (sau un kit de administrare, dacă există) pentru mai multe informații privind crearea fișierelor de configurare pentru clienți.

Rezumat

Un server intermediar poate fi folosit pentru izolarea clienților de rețeaua externă. Ascunzând informațiile despre clienți și rețea, serverul intermediar face mai dificilă sarcina hackerilor. În acest capitol am prezentat un produs popular: Microsoft Proxy Server. Acesta nu este singurul server intermediar disponibil pe piață, dar, datorită popularității platformelor Windows, probabil că acesta este produsul pe care îl veți întâlni cel mai des pentru o vreme, mai ales că are în spate o companie mare care asigură asistența tehnică.

Firewall-ul Elron CommandView

- Prezentare generală
- Instalarea firewall-ului CommandView
- Aplicația de gestionare a firewall-ului CommandView
- Gestionarea serviciilor pentru utilizatori
- Ce altceva puteți încerca

Prezentare generală

Elron CommandView Firewall este un firewall flexibil și ușor de gestionat, care poate fi folosit într-o rețea mare sau mică pentru crearea unei conexiuni sigure la Internet. Pachetul CommandView este format dintr-un serviciu firewall și o aplicație de gestionare separată, rulată pe același calculator sau pe o altă gazdă. Pe lângă serviciile de rețea de bază, cum ar fi FTP și e-mail, CommandView vă permite să puneți la dispoziție multe alte servicii și chiar să configurați un serviciu propriu, dacă nu găsiți ceea ce aveți nevoie în lista predefinită a firewall-ului.

Încercați mai întâi

Evaluati produsul înainte de a-l cumpăra. Puteți descărca o versiune de probă a firewall-ului CommandView de la următoarea adresă Web:

www.elronsoftware.com

Acest capitol prezintă principalele etape pentru instalarea serviciului firewall și a aplicației de gestionare și vă arată cum să configurați serviciile de bază. Discutarea tuturor opțiunilor de configurare și a serviciilor oferite de firewall-ul CommandView ar umple o carte întreagă, așa că acest capitol ar trebui să fie considerat doar o introducere. De exemplu, pe lângă asigurarea unui număr mare de servicii de rețea, CommandView vă permite să folosiți translatarea adreselor de rețea (NAT – Network Address Translation) sau rețele virtuale private (VPN – Virtual Private Network) pentru crearea unui canal de comunicații sigur și criptat într-o rețea nesigură, cum ar fi Internetul. Deoarece CommandView se bazează pe un standard din domeniu, veți vedea că poate fi configurat astfel încât să

opereze cu produsele altor furnizori. De exemplu, CommandView acceptă protocoalele IP Authentication Header și Encapsulating Security Payload (ESP).

Ar trebui să cumpărați firewall-ul Elron CommandView?

Chiar de la început, ar trebui să menționez că nu am ales firewall-ul Elron CommandView ca exemplu în această carte pentru a vă recomanda să îl cumpărați. Mai degrabă aș dori ca dumneavoastră să folosiți informațiile din carte pentru a lua propriile decizii inteligente de achiziție. Există sute de produse similare din care puteți alege. Deși nu susțin anume produsul companiei Elron, l-am ales pentru că este reprezentativ pentru multe alte produse care pot fi ușor instalate, configurate și gestionate. Totuși, aș vrea să le mulțumesc celor de la Elron pentru ajutorul pe care mi l-au dat răspunzând la câteva dintre întrebările mele în momentul scrierii acestui capitol.

Vezi și

➤ Pentru mai multe informații despre protocoalele IP Authentication Header și Encapsulating Security Payload (ESP), vezi capitolul 10, „Rețele virtuale private (VPN) și tuneluri”, la pagina 175.

Vezi și

➤ Pentru mai multe informații despre translatarea adreselor de rețea (NAT – Network Address Translation), vezi capitolul 7, „Porți de aplicații și servere intermediar”, la pagina 132.

Instalarea firewall-ului CommandView

Pentru instalarea firewall-ului CommandView, aveți nevoie de un calculator Windows NT 4.0 (versiunea curentă nu este compatibilă cu Windows 2000) pe care este instalat cel puțin Service Pack 3. Sistemul care rulează serviciul Firewall SMLI Engine ar trebui să fie echipat cu următoarele componente:

- Un procesor Pentium la cel puțin 166 MHz
- Cel puțin 64 MB de memorie (128 MB este mai bine)
- 500 MB de spațiu liber pe disc
- Două adaptoare de rețea (la 10 Mb, 100 Mb sau 10/100 Mb)

Dacă vreți să creați și o zonă demilitarizată (DMZ), aveți nevoie de trei adaptoare de rețea.

Vezi și

➤ Pentru mai multe informații despre folosirea unei zone demilitarizate, vezi capitolul 4, „Politici de securitate pentru firewall-uri și strategii de protecție a firewall-urilor”, la pagina 75.

Puteți rula și aplicația Firewall Manager pe același sistem. O altă soluție este să instalați aplicația de gestionare pe un alt sistem Windows NT 4.0, Windows 95 sau Windows 98. Dacă optați pentru folosirea unui alt calculator pentru aplicația de gestionare, asigurați-vă că ambele gazde se află pe același segment de rețea și în aceeași subrețea IP. Rețineți că este o practică bună de securitate să instalați dispozitivele firewall într-un loc sigur – cum ar fi un cabinet încuiat sau o sală de calcul – ceea ce presupune, logic, instalarea aplicației de gestionare pe un alt calculator, mai accesibil. Cerințele minime pentru sistemul pe care este rulată aplicația de gestionare sunt următoarele:

- Windows 95, Windows 98 sau Windows NT 4.0
- 32 MB de memorie
- 50 MB de spațiu liber pe disc
- Stivă TCP/IP compatibilă cu WinSock 2.0

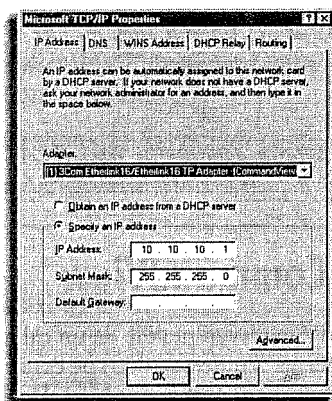
Înainte de a lansa în execuție programul de instalare, ar trebui să verificați plăcile de rețea instalate în sistem și să notați numerele alocate acestora.

Verificarea plăcilor de rețea

1. Selectați comanda Start, Settings, Control Panel. Executați dublu clic pe miniaplicația Network.

FIGURA 19.1

Folosiți meniul derulant Adapter pentru vizualizarea și înregistrarea adaptoarelor instalate în sistem.



2. Executați clic pe eticheta Protocols, apoi evidențiați opțiunea TCP/IP Protocol. Executați clic pe butonul Properties.
3. În pagina de proprietăți a protocolului TCP/IP (figura 19.1) puteți vedea meniul derulant cu eticheta Adapter. În acest meniu ar trebui să existe un articol pentru fiecare adaptor de rețea din sistem. Executați clic pe săgeata în jos din meniu pentru a vedea fiecare adaptor și notați numerele asociate cu acestea.

Rularea programului de instalare

Pentru lansarea programului de instalare, introduceți în unitate CD-ul CommandView. Programul de instalare ar trebui să pornească automat. O altă soluție este să rulați manual programul, lansând în execuție programul SETUP.EXE, dacă CD-ul este încărcat pe o unitate de rețea.

Rularea programului de instalare

1. Primele ecrane prezintă informații despre condițiile de instalare și acordarea licenței. După ce citiți aceste ecrane, puteți executa clic pe butonul Next sau Yes pentru a continua.
2. Următoarea casetă de dialog (figura 19.2) vă cere să alegeți tipul instalării. Opțiunea Typical instalează atât serviciul firewall, cât și aplicația de gestionare. Selectați opțiunea Custom dacă vreți să instalați numai serviciul sau numai aplicația de gestionare. Apare o casetă de dialog de întâmpinare. Executați clic pe butonul Next pentru a continua.
3. Apare o casetă de dialog care vă cere să introduceți directorul în care se va face instalarea. Acceptați directorul prestabilit sau schimbați-l, apoi executați clic pe butonul Next pentru a continua.

FIGURA 19.2

Selectați opțiunea Typical pentru a instala serviciul firewall și aplicația de gestionare.

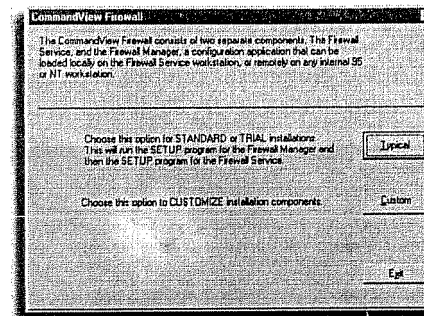
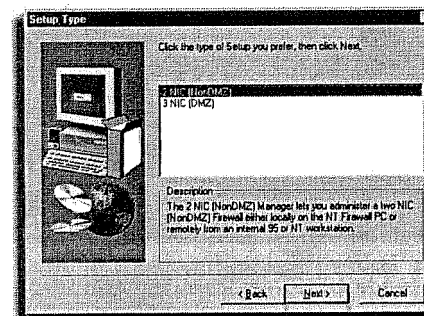


FIGURA 19.3

Puteți instala firewall-ul CommandView folosind două sau trei adaptoare de rețea.



4. Casetă de dialog Setup Type (figura 19.3) vă cere să specificați tipul de arhitectură pentru firewall-ul pe care vreți să îl creați, folosind fie două adaptoare de rețea pentru un firewall de bază, fie trei adaptoare de rețea pentru crearea unei zone demilitarizate (DMZ). Pentru această instalare demonstrativă, am selectat opțiunea cu două adaptoare de rețea.
5. Apare o casetă de dialog numită Select Program Folder. Executați clic pe butonul Next pentru a continua, dacă doriți să folosiți opțiunea prestabilită, care creează un do-

sar numit Elron CommandView, sau selectați un dosar existent și executați clic pe butonul Next.

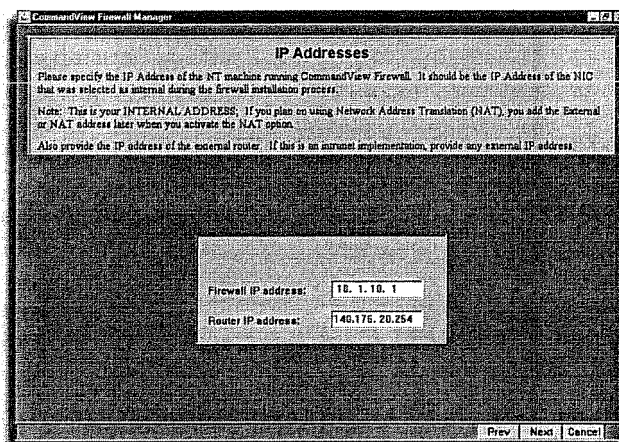
6. Casetă de dialog Setup Complete vă informează că a fost instalată aplicația de gestionare. Executați clic pe butonul Finish. Dacă la începutul procesului ați optat pentru instalarea ambelor aplicații, programul începe acum instalarea serviciului firewall.
7. Prima casetă de dialog pentru instalarea serviciului vă cere din nou să alegeți tipul firewall-ului: cu două sau cu trei adaptoare de rețea. Selectați același tip pe care l-ați ales pentru aplicația de gestionare.
8. O altă casetă de dialog vă cere să specificați destinația instalării componentelor software ale firewall-ului. Acceptați dosarul prestabilit sau schimbați-l, apoi executați clic pe butonul Next pentru a continua.
9. Următoarea casetă de dialog conține lista adaptoarelor de rețea din sistem. Folosiți cursorul mouse-ului pentru a trage și plasa fiecare adaptor din listă în locul corespunzător din arhitectura firewall-ului. De exemplu, dacă primul adaptor este cel conectat la rețeaua internă, trageți-l peste pictograma numită Internal Network. După ce terminați, executați clic pe butonul Save. Când programul de instalare vă cere acest lucru, reîncărcați calculatorul.

După reîncărcarea calculatorului și conectarea la rețea, apare o casetă de dialog numită New Firewall Installation, care vă ghidează în restul procesului de configurare a firewall-ului. Nu este nevoie să configurați aplicația de gestionare, așa că, dacă ați instalat numai această aplicație, nu și serviciul firewall propriu-zis, executați clic pe butonul Cancel. În caz contrar, pentru a continua configurarea, executați clic pe butonul Next.

Programul wizard vă ghidează în procesul de configurare a politicilor pentru diferite servicii populare, cum ar fi WWW, e-mail și FTP. Totuși, mai întâi trebuie să configurați unul sau mai multe domenii de adrese din rețeaua internă, care vor fi grupate în cadrul politicilor stabile. În figura 19.4 puteți vedea caseta de dialog folosită în acest scop.

FIGURA 19.4

Folosiți această casetă de dialog pentru a crea unul sau mai multe domenii de adrese.



Pentru fiecare serviciu, puteți decide ce tip de acces veți permite. De exemplu, pentru serviciul WWW puteți activa sau dezactiva accesul către exterior pentru toate adresele incluse în domeniile de adrese create pentru adaptorul de rețea intern. Dacă preferați, puteți crea o politică proprie care vă permite să specificați adrese IP individuale pentru care este permis accesul. Celelalte servicii sunt configurate într-o manieră similară, cu casete de dialog specifice fiecărui serviciu.

Pe lângă configurarea politicilor pentru serviciile de rețea, programul wizard vă permite să configurați informările prin e-mail pentru evenimentele semnificative detectate de firewall. În figura 19.5 puteți vedea caseta de dialog Set Notification Command. Dacă vreți să activați informările prin e-mail, marcați caseta Enable E-mail notification. Dacă nu vreți ca programul să vă informeze prin e-mail, lăsați liberă această casetă de validare. Celelalte câmpuri vă permit să introduceți informațiile necesare, cum ar fi adresa serverului de poștă electronică. De asemenea, puteți specifica adresa de poștă electronică ce va apărea ca expeditor al informărilor prin e-mail. În exemplul din figura 19.5, aici a fost selectată adresa ogletree@twoinc.

Executați clic pe butonul Add Email ID. O altă casetă de dialog, numită Create Email Rule (vezi figura 19.6), vă cere să introduceți adresa de e-mail la care vor fi trimise informările și vă permite să selectați nivelul de severitate de la care vreți să fiți informat. Evenimentele cu acest nivel de severitate sau cu un nivel superior vor fi trimise către adresa specificată. Executați clic pe butonul OK ca să adăugați contul și să vă întoarceți la caseta de dialog anterioară.

Puteți continua să configurați unul sau mai multe conturi de e-mail în această casetă de dialog, executând clic pentru fiecare pe butonul Add Email ID (vezi figura 19.5).

FIGURA 19.5

Introduceți numele sau adresa serverului de poștă electronică și numele contului e-mail de la care vor fi trimise informările.

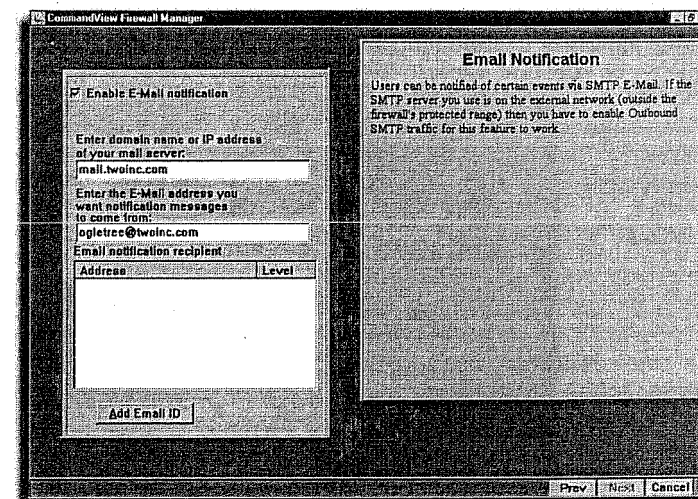
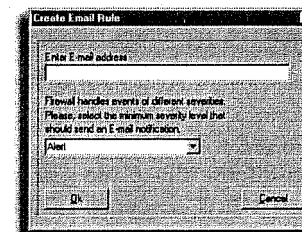


FIGURA 19.6

Introduceți contul de e-mail care va primi informările și selectați nivelul de severitate.



După terminarea procesului de configurare, vi se cere să salvați configurația creată și să activați firewall-ul. Nu vă faceți probleme dacă în acest moment nu știți cu exactitate cum vreți să configurați firewall-ul. Programul wizard este util pentru o configurare rapidă a firewall-ului după instalare, dar puteți să reveniți oricând, folosind utilitarul de gestionare, și să luați alte decizii de configurare.

Aplicația de gestionare a firewall-ului CommandView

Serviciul firewall și aplicația de gestionare sunt programe separate. Puteți să le rulați pe același calculator sau pe calculatoare diferite. Deși serviciul firewall poate fi rulat numai pe un calculator Windows NT, aplicația de gestionare poate fi rulată pe o stație de lucru cu sistem de operare Windows NT sau Windows 95/98. Aplicația de gestionare este folosită pentru a controla firewall-ul. De exemplu, dacă decideți ulterior să schimbați politicile de securitate create inițial, o puteți face cu ajutorul acestui program.

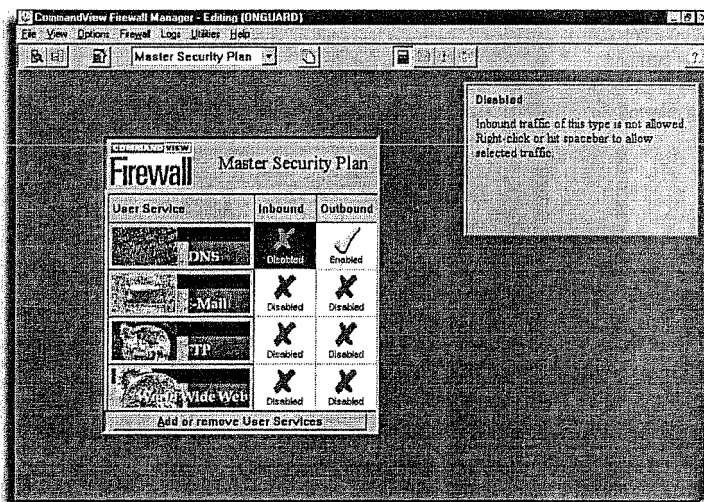
La prima lansare a aplicației de gestionare, vi se cere să specificați firewall-ul la care va fi atașată aplicația și o parolă pentru firewall. Puteți folosi aplicația de gestionare pentru a controla mai multe instalări ale serviciului firewall, așa că mai întâi trebuie să selectați firewall-ul pe care vreți să îl gestionați în momentul respectiv. La prima rulare a programului pentru un anumit firewall, ar trebui să selectați caseta de validare Default Password. În timpul rulării programului, puteți specifica o parolă proprie pentru a proteja programul împotriva utilizatorilor neautorizați.

În figura 19.7 puteți vedea aplicația de gestionare, care afișează planul principal de securitate (Master Security Plan) salvat anterior. Aceasta este configurația pe care ați

creat-o cu ajutorul programului wizard de instalare sau configurația curentă, dacă ați folosit deja aplicația de gestionare pentru efectuarea unor modificări.

FIGURA 19.7

Aplicația CommandView Firewall Manager este folosită pentru a controla serviciul firewall.



Meniurile File și View

Meniul File (Fișier) vă permite să executați diferite funcții de gestionare. Tabelul 19.1 prezintă opțiunile de meniu, împreună cu o scurtă descriere a modului de folosire a acestora.

Tabelul 19.1 Opțiuni pentru gestionarea fișierelor

Opțiune de meniu	Descriere
Attach to Firewall	Atașează programul la un anumit firewall în vederea gestionării.
Detatch from Firewall	Întrerupe conexiunea curentă cu un firewall.
Configure New Firewall	Lansează procesul de configurare rapidă a unui nou firewall.
Retrieve Plan from Firewall	Obține fișierul de plan pentru firewall-ul activ în momentul respectiv.
Save Plan to Firewall	Salvează configurația curentă în firewall, ca plan principal de securitate. Pentru ca planul să aibă efect, trebuie să reporniți firewall-ul.
Load Plan from File	Încarcă o configurație salvată (un fișier cu extensia .OGM)
Save Plan to File	Salvează o configurație într-un fișier (cu extensia .OGM)

Opțiune de meniu	Descriere
Print MSP Summary	Tipărește un rezumat al planului principal de securitate (MSP – Master Security Plan), prezentând serviciile de utilizator și permisiunile de acces din și către exterior.
Print MSP Details	Tipărește o listă detaliată a planului principal de securitate.
Exit	Iese din aplicația Firewall Manager.

Planul principal de securitate

Opțiunile pe care le specificați pentru planul principal de securitate sunt stocate într-un fișier. Puteți crea mai multe planuri. Această posibilitate este convenabilă dacă vreți să testați o anumită configurație și să o salvați pentru testarea sau studierea ulterioară. Fiecare configurație este salvată într-un fișier cu extensia .OGM. Planul principal de securitate, care este configurația rulată în momentul respectiv de firewall, este salvat într-un fișier numit ONGUARD. OGM, aflat în directorul C:\Program Files\Elron Software\FirewallManager\Onguard. Dacă salvați mai multe configurații, acestea sunt păstrate în mod prestabilit în acest director, dar puteți specifica un alt director dacă doriți.

După cum puteți vedea, acest meniu vă permite să executați câteva funcții de bază, cum ar fi schimbarea firewall-ului gestionat. Folosiți opțiunile Attach și Detach pentru a trece de la un firewall la altul. Opțiunile de încărcare și salvare vă permit să vedeți configurația planului rulat de firewall în momentul respectiv sau să gestionați alte configurații și să le salvați într-un fișier. Dacă vreți să schimbați planul principal de securitate, folosiți opțiunea Save Plan to Firewall, apoi folosiți meniul Firewall pentru a reporni firewall-ul, astfel încât planul să aibă efect.

Meniul View conține și mai multe opțiuni, permițându-vă să afișați planul principal de securitate, pe scurt și în detaliu, sau să îl salvați într-un fișier de text care poate fi apoi tipărit. Alte opțiuni vă permit să editați domeniile de adrese, să selectați metodele de criptare, să gestionați cheile de criptare și așa mai departe. Tot în acest meniu puteți opta pentru adăugarea sau modificarea comenzilor de informare, astfel încât să fiți avertizat atunci când apar evenimente semnificative.

Opțiuni din meniul Firewall

Meniul Firewall conține doar câteva opțiuni. Tabelul 19.2 prezintă aceste opțiuni, împreună cu o scurtă descriere a modului de folosire.

Tabelul 19.2 Opțiunile din meniul Firewall

Opțiune de meniu	Descriere
Set Date/Time	Permite stabilirea datei și a orei.
Set Password	Folosiți această opțiune ca să schimbați parola pentru serviciul firewall pe care îl gestionați.

continuare

Tabelul 19.2 Continuare

Opțiune de meniu	Descriere
SMXP Encryption Key	Dacă nu specificați aici o cheie proprie, firewall-ul folosește pentru criptare o cheie prestabilită.
Check Alive	Această opțiune verifică dacă firewall-ul este activ în momentul respectiv.
Ping Router	Folosiți această opțiune pentru a determina dacă firewall-ul poate lua legătura cu poarta prestabilită sau cu ruterul extern care asigură conexiunea la Internet.
ReStart	Repornește firewall-ul pe care îl gestionați. Rețineți că această opțiune determină reincărcarea calculatorului, dar puteți specifica momentul în care se face acest lucru.
Upgrade	Această opțiune este folosită pentru modernizarea firewall-ului, după ce ați modernizat aplicația de gestionare. După lansarea acestei comenzi este necesară reincărcarea sistemului.

Opțiunile pe care probabil le veți folosi cel mai des sunt Set Password și ReStart. Rețineți că atunci când vă conectați pentru prima dată la un serviciu firewall nou instalat, nu este stabilită nici o parolă. Din acest motiv ați selectat caseta de validare Default Password. Imediat după instalarea unui nou firewall, intrați în acest meniu și specificați o parolă. Chiar dacă rulați aplicația de gestionare pe un calculator pe care îl considerați sigur, ar trebui să vă intereseze această parolă. De ce? Deoarece parola este aplicată serviciului firewall, nu programului de gestionare sau calculatorului pe care este rulat acesta. Dacă nu stabiliți o parolă, ar fi simplu pentru cineva cu cunoștințele necesare să obțină o copie a aplicației de gestionare, să o instaleze pe un alt calculator, să atașeze aplicația la serviciul firewall (folosind parola prestabilită) și să facă modificări.

Stabiliți imediat parola! Schimbați-o frecvent! Desigur, la fel ca pentru toate parolele, alegeți o parolă bună și nu o scrieți pe nimic!

Opțiuni din meniul Logs

Acest meniu este folosit pentru examinarea fișierelor jurnal păstrate de serviciul firewall. Fișierele jurnal sunt Events, Traps și Statistics. După ce selectați unul dintre aceste jurnale, puteți folosi celelalte opțiuni pentru sortarea înregistrărilor din jurnal sau pentru crearea filtrelor, astfel încât să obțineți numai informațiile care vreți să fie păstrate în fișierele jurnal. Opțiunile Sort și Filter devin disponibile numai după ce selectați fișierul jurnal pe care vreți să îl gestionați.

Gestionarea serviciilor pentru utilizatori

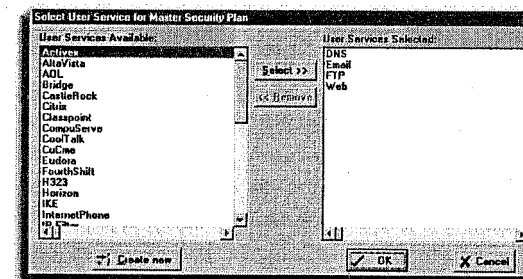
Mai devreme în acest capitol, a fost folosit un program wizard de configurare pentru crearea politicii inițiale a firewall-ului pentru serviciile de bază. Firewall-ul CommandView nu este limitat la serviciile WWW, FTP sau e-mail. De fapt, firewall-ul vă permite să oferiți mai mult de 25 de servicii predefinite. De asemenea, dacă nu găsiți ceea ce vă interesează, puteți să creați un nou serviciu pentru utilizatori. Printre serviciile predefinite se numără următoarele:

- AOL
- Citrix
- CompuServe
- IPX
- IRC
- LDAP
- NetBIOS
- News

După cum vedeți, serviciile care pot fi folosite cu firewall-ul CommandView acoperă o gamă largă. Găsiți servicii obișnuite, cum ar fi FTP, e-mail și news, precum și servicii pentru IPX și LDAP. Dacă în rețea aveți servere Novell, puteți permite accesul la acestea prin firewall. Dacă sunteți în curs de modernizare a rețelei cu servere Windows 2000, puteți investiga configurarea serviciului LDAP pentru firewall, deoarece LDAP este principalul protocol pentru cablu folosit pentru accesul la Active Directory.

FIGURA 19.8

Folosind această casetă de dialog selectați serviciile pe care vreți să le adăugați în planul principal de securitate.



jos a ferestrei aplicației de gestionare, atunci când lansați pentru prima dată aplicația. Casetă de dialog Select User Service for Master Security Plan (vezi figura 19.8) vă permite apoi să selectați serviciul și să îl adăugați la plan. Evidențiați serviciul pe care vreți să îl adăugați, apoi executați clic pe butonul Select. Serviciul apare în lista User Services Selected din partea dreaptă a casetei de dialog.

Pentru eliminarea unui serviciu din plan, evidențiați-l și executați clic pe butonul Remove. De asemenea, puteți executa dublu clic pe un serviciu pentru a-l adăuga sau a-l scoate din plan, în funcție de starea curentă. După ce terminați gestionarea serviciilor, executați clic pe butonul OK. Planul principal de securitate prezintă acum noua configurație de servicii. Dacă ați adăugat un nou serviciu, acesta este dezactivat până la stabilirea unei politici.

Pentru adăugarea unuia dintre aceste servicii la planul principal de securitate al firewall-ului, executați clic pe butonul Add or Remove User Services. Acest buton apare în partea de

Ce altceva puteți încerca

CommandView este un exemplu bun de produs comercial tipic pentru firewall-uri. Dacă vreți să continuați investigațiile, vizitați situl Web al companiei Elron, menționat la începutul acestui capitol, descărcați o copie de evaluare și instalați produsul. De fapt, dacă faceți acum primii pași în domeniul firewall-urilor, probabil că ar fi o idee bună să căutați și alte produse și, pentru cele care oferă o versiune de evaluare, să faceți același lucru. De fiecare dată când parcurgeți procesul de instalare și gestionare a unui produs, aflați mai multe lucruri despre caracteristicile ce pot fi folosite cel mai bine în mediul dumneavoastră. Încercați să descărcați câteva produse. Puteți folosi copiile de evaluare ca să faceți prezentări pentru șefii și colaboratorii dumneavoastră care vor lucra cu produsele software pentru firewall-uri.

Rezumat

Firewall-ul Elron CommandView este un exemplu bun de produs comercial complet. Dacă nu îndrăzniți să abordați configurarea unui firewall folosind utilitare precum TCP Wrappers sau TIS Internet Firewall Toolkit, un produs precum Elron este foarte bun. Atunci când decideți ce produse veți folosi pentru crearea unui firewall, trebuie să luați în considerare câțiva factori. Desigur, unul dintre cei mai importanți factori este dacă produsul va asigura serviciile de rețea de care aveți nevoie. Un factor la fel de important este asistența pe care o oferă furnizorul. Elron, la fel ca multe alte produse comerciale pentru firewall-uri, este susținut de un furnizor care asigură asistență tehnică de calitate. Ca urmare, dacă nu dispuneți de personal experimentat care să se ocupe de detaliile fișierelor de configurare sau de compilare, o soluție precum Elron CommandView Firewall este o alegere bună.

Capitolul 20

Dispozitive firewall

- Ce este un dispozitiv firewall?
- Evaluarea prețului unui dispozitiv firewall

Ce este un dispozitiv firewall?

În toată această carte, firewall-urile au fost considerate sisteme complexe, care folosesc filtrarea pachetelor, porți la nivel de aplicație și de circuit, autentificare puternică și alte tehnici pentru protejarea rețelei. În unele capitole, ați fost avertizat să nu încercați să instalați un anumit produs (cum ar fi TIS Internet Firewall Toolkit) decât dacă aveți cunoștințe aprofundate despre administrarea unui sistem UNIX și despre TCP/IP. Cele mai multe dintre componentele pentru firewall-uri și utilitarele de securitate ce pot fi descărcate gratuit din Internet trebuie să fie compilate pe sistemul local, apoi trebuie să pierdeți timp cu modificarea detaliilor de configurare.

Pentru o companie destul de mare ca să susțină un personal numeros de gestionare a rețelei și a utilizatorilor, probabil că gestionarea unui firewall nu înseamnă mare lucru. Nu este nevoie decât ca una sau mai multe persoane care au cunoștințele necesare să preia responsabilitatea monitorizării și întreținerii firewall-ului. Într-o companie mică sau într-un birou care nu are decât unul sau două servere, câteva stații de lucru și o conexiune la Internet, s-ar putea să nu fie posibilă din punct de vedere financiar angajarea unei persoane care să nu facă altceva decât să gestioneze un firewall. Într-un asemenea mediu, probabil că toate aplicațiile sunt produse comerciale, iar angajații nu au cunoștințe aprofundate de programare sau de gestionare a sistemelor.

Într-o asemenea situație, cum puteți să vă conectați în siguranță la Internet? Este necesar ca o companie mică să rămână dependentă de furnizorul de servicii Internet pentru toate cerințele de securitate?

În ultima vreme, un nou tip de firewall-uri se bucură de atenția presei. Pentru aceste soluții complete de securitate în Internet a fost inventat termenul *dispozitive firewall (firewall appliances)*. Numeroasele produse considerate a face parte din această nouă clasă de firewall-uri variază considerabil ca preț, eficiență și caracteristici. Totuși, cele mai multe dintre produsele considerate a fi dispozitive firewall au următoarele caracteristici:

- Instalare rapidă și simplă. Unii furnizori susțin chiar că produsele lor asigură caracteristici plug-and-play.
- Interfață simplă de gestionare; eventual chiar posibilități de gestionare de la distanță.
- Sunt dispozitive independente.

- Funcționează cu interfețe multiple, de la linii telefonice comutate la Ethernet și, posibil, linii T1.
- Politici de securitate prestabilite, astfel încât utilizatorii nu trebuie neapărat să înțeleagă toate detaliile.
- Funcționalitate de filtrare a pachetelor și intermediere a aplicațiilor.
- Funcționalitate de traducere a adreselor de rețea (NAT – Network Address Translation).
- Posibilități de raportare ușor de folosit, de obicei cu un set de rapoarte predefinite. Posibilități de avertizare.
- Posibilități de lucru în rețele virtuale private (VPN – Virtual Private Networking).
- Asistență corespunzătoare din partea furnizorilor.

Dispozitive firewall mari și mici

Deși piața dispozitivelor firewall se va dezvolta puternic în următorii ani, pe măsură ce firmele mici încep să le folosească pentru conexiunile la Internet, există o piață și pentru sistemele performante, independente și ușor de gestionat. De exemplu, Cisco și Lucent oferă produse care sunt considerate dispozitive firewall, dar care costă mai mult de 10.000 de dolari. Evident, aceste „dispozitive” nu sunt destinate micilor companii. Ținta acestor produse sunt administratorii de rețea care gestionează rețele mari. Deși termenul *dispozitive firewall* sugerează faptul că acestea sunt aparate la fel de simple ca un prăjitor de pâine, nu înseamnă că sunt dispozitive ieftine, la îndemâna oricui. Termenul „dispozitiv” nu se referă la preț, ci la ușurința în folosire.

Instalare rapidă și simplă

Una dintre cele mai profitabile caracteristici ale dispozitivelor firewall, din punct de vedere comercial, este instalarea ușoară. Utilizatorul ar trebui doar să-și conecteze rețeaua la una dintre interfețele dispozitivului firewall, să lege conexiunea Internet la cealaltă interfață și să răspundă la câteva întrebări simple. Nu ar trebui să fie necesară editarea unor fișiere de configurare complicate. Nu este necesar ca utilizatorul să știe în detaliu modul de funcționare a adresării IP sau cum să împartă în subrețele o adresă de rețea. Configurarea ar trebui să fie făcută de un program de asistență (wizard) care să îi pună utilizatorului câteva întrebări simple.

Procesul de configurare ar trebui să vă permită să specificați, într-o manieră generală, o politică de securitate pentru rețea. Întregul proces de instalare, pentru cele mai multe dispozitive, de la despachetare până la utilizarea dispozitivului, nu ar trebui să dureze mai mult de o oră. Dacă timpul necesar pentru instalarea firewall-ului depășește o oră, probabil că numele de dispozitiv firewall nu este potrivit.

Interfață simplă de gestionare

După terminarea instalării, nu ar trebui să faceți prea multe lucruri pentru gestionarea dispozitivului. Multe dispozitive firewall nu au nici măcar o consolă de sistem – un monitor. Tendința este de a folosi posibilități de gestionare de la distanță. Calea obișnuită este o interfață Web bazată pe HTML, dar asigurați-vă că între dispozitivul firewall și consola de gestionare este folosit un canal de comunicații criptat. În acest scop, dispozitivul ar trebui să fie compatibil cu o formă standardizată de criptare, cum ar fi DES sau SSL (Secure Sockets Layer).

Interfața ar trebui să fie grafică. O interfață în linie de comandă, cu sintaxă complexă și linii lungi de comenzi criptice, nu este o modalitate de lucru potrivită pentru un dispozitiv simplu de acest tip. Cele mai multe acțiuni ar trebui să poată fi executate cu ajutorul mouse-ului. Producerea unui raport ar trebui să se reducă la selectarea unei comenzi dintr-un meniu și, eventual, introducerea unei date calendaristice sau a altor informații care vor fi folosite pentru generarea raportului.

Dispozitive independente

Pentru a îndeplini cerințele specificațiilor plug-and-play, un dispozitiv firewall este conținut într-o singură cutie, de dimensiunea unui PC obișnuit sau mai mică. De fapt, unele platforme hardware pentru dispozitivele firewall sunt chiar PC-uri care folosesc fie un sistem de operare propriu, fie o versiune îmbunătățită a unui sistem de operare standard. De exemplu, dispozitivul firewall Interceptor, al companiei Technologic, folosește un sistem de operare bazat pe BSD/OS, produs de Berkeley Software Design, Inc. (BSDI). Acesta este un sistem de operare de tip UNIX. Dispozitivul Lucent Managed Firewall folosește sistemul de operare Inferno al companiei Lucent, care conține codul pentru funcțiile firewall-ului.

Există câteva produse care folosesc un sistem de operare conținut pe o dischetă sau pe un CD-ROM. Prin folosirea unui CD-ROM cu acces numai pentru citire, vă asigurați că fișierele sistemului de operare folosite de dispozitivul firewall nu pot fi suprascrise. Există câteva dispozitive care duc mai departe această idee. Dispozitivul firewall PERMIT al companiei TimeStep nu are componente în mișcare. Acest dispozitiv firewall bazat pe circuite semiconductoare păstrează sistemul de operare în memorie, împreună cu o versiune a programului Check Point Firewall-1.

Atunci când evaluați produse similare, nu uitați că unul dintre scopurile proiectării dispozitivelor firewall este simplitatea, așa că nu ar trebui să existe manuale complicate care să vă explice ce decizii trebuie să luați pentru instalarea componentelor software.

Interfețe de rețea multiple

Într-un mediu restrâns, conexiunea la Internet se face, probabil, printr-o linie telefonică comutată, ISDN, sau chiar o linie DSL (Digital Subscriber Line). Cele mai multe dispozitive firewall pot lucra cu oricare dintre aceste conexiuni. Modelele performante, cu prețuri mai ridicate, includ conexiuni pentru linii T1. Verificați în detaliu documentația furnizorului, pentru a vă asigura că dispozitivul pe care îl cumpărați poate fi legat la rețeaua dumneavoastră și la conexiunea Internet, fără să necesite adaptoare speciale sau alte componente hardware.

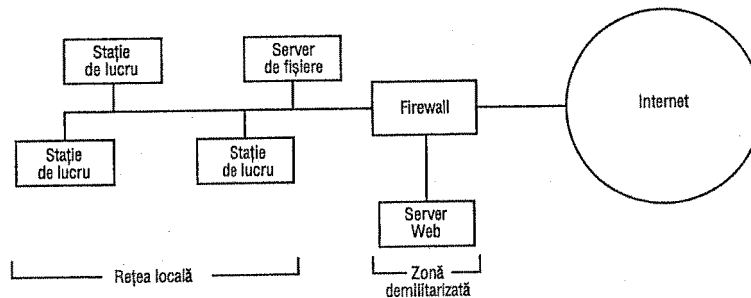
Deși în maniera tipică de instalare a unui firewall într-un mic birou sunt folosite numai două interfețe, unele dispozitive firewall vă pun la dispoziție încă o interfață, care poate fi folosită pentru o „zonă demilitarizată”, așa cum se poate vedea în figura 20.1.

Această caracteristică este importantă dacă organizația dumneavoastră gestionează un server Web propriu. Deși tendința actuală este de a folosi o sursă externă ca gazdă pentru un sit Web, aceasta ar putea să nu fie cea mai potrivită soluție pentru compania

dumneavoastră. Întreținerea unui sit Web simplu, folosind instrumentele de dezvoltare moderne, nu trebuie să fie un proces mare consumator de timp, implicând o mulțime de programatori experimentați. Aplicații precum Microsoft FrontPage pot fi folosite atât pentru crearea unor situri Web foarte complexe, cât și a unora simple și ușor de gestionat. Dacă dispozitivul firewall vă oferă opțiunea de separare a serverului Web (sau a unui alt server care pune la dispoziție un serviciu de rețea), puteți îmbunătăți mult securitatea rețelei locale, conectată la celălalt adaptor al firewall-ului.

FIGURA 20.1

O a treia interfață de rețea vă permite să amplasați servere într-o „zonă demilitarizată” (DMZ).



Politici de securitate prestabilite

În capitolul 4, „Politici de securitate pentru firewall-uri și strategii de proiectare a firewall-urilor”, ați învățat că înainte de a putea să implementați un firewall, trebuie să elaborați o politică de securitate a sitului, apoi o politică de securitate a firewall-ului propriu-zis. Deși un dispozitiv firewall nu elimină toate detaliile implicate de acest proces, poate să le simplifice. Folosirea unui program wizard pentru configurarea firewall-ului face ca procesul inițial de instalare să devină o sarcină simplă. Câteva dintre dispozitivele firewall pe care le-am văzut în ultima vreme includ un set de politici de securitate descrise într-un limbaj simplu, în locul unui limbaj tehnic complicat. Utilizatorul poate să decidă rapid ce politică de securitate va folosi, lăsând apoi programul wizard să configureze regulile corespunzătoare pentru firewall.

Dispozitivul Lucent Managed Firewall vă permite să creați *zone virtuale de securitate* pentru diferite grupuri de gazde, astfel încât fiecărui grup să îi poată fi aplicată o anumită politică de securitate. Acest lucru poate fi făcut cu un singur dispozitiv firewall sau cu un grup de dispozitive gestionate centralizat. Dacă o politică de securitate este modificată, schimbările pot fi propagate imediat către toate dispozitivele gestionate din același punct.

Dacă nu aveți timp să aprofundați complicațiile legate de reguli, servicii, numere de porturi și așa mai departe, existența unui set predefinit de politici de securitate ușor de înțeles este un avantaj.

Filtrarea pachetelor și intermedierea aplicațiilor

Un firewall bun asigură atât funcții de filtrare a pachetelor, cât și de intermediere a aplicațiilor. Verificați dacă serviciile de rețea pe care le folosiți sunt incluse ca aplicații intermediar pentru dispozitivul respectiv. De asemenea, pentru celelalte servicii ar trebui să fie

prevăzută o funcție de poartă generică la nivel de circuit. Posibilitățile de filtrare a pachetelor ar trebui să fie implementate folosind tehnici de filtrare a pachetelor dependente de stare. Desigur, nu mai este nevoie să menționăm că un dispozitiv firewall modern pune la dispoziție aceste servicii într-o modalitate transparentă pentru client.

Vezi și

- Pentru mai multe informații despre filtrarea pachetelor, vezi capitolul 5, „Filtrarea pachetelor”, la pagina 95.
- Pentru mai multe informații despre modul de funcționare a serverelor intermediar, vezi capitolul 7, „Porți de aplicații și servere intermediar”, la pagina 132.

Translatarea adreselor de rețea (NAT – Network Address Translation)

Furnizorul dumneavoastră de servicii Internet folosește protocolul DHCP pentru a vă aloca dinamic o adresă IP pentru conexiunea Internet, sau aveți o subrețea dedicată de adrese valabile în Internet? Dacă folosiți o conexiune pe linii telefonice comutate, probabil că este utilizat protocolul DHCP. În acest caz, nu aveți garanția că vi se alocă aceeași adresă IP la fiecare apel, așa că dispozitivul firewall trebuie să aibă posibilitatea de a se adapta. Asigurați-vă că dispozitivul nu vă cere să alocați static o adresă adaptorului conectat la Internet. Pentru o conexiune pe linii comutate de acest tip, asigurați-vă că dispozitivul este compatibil cu protocolul PPP.

Vezi și

- Translatarea adreselor de rețea este prezentată cu mai multe detalii în secțiunea „Translatoare de adrese de rețea (NAT)”, în capitolul 7, „Porți de aplicații și servere intermediar”, la pagina 139.

Dacă nu aveți o subrețea dedicată de adrese pe care să le folosiți pentru a aloca informațiile de configurare IP stațiilor de lucru din rețeaua locală, trebuie să utilizați unul dintre domeniile de adrese private rezervate de organizația IANA în acest scop. Aceasta înseamnă că dispozitivul firewall trebuie să accepte translatarea adreselor de rețea (NAT – Network Address Translation), astfel încât clienții din rețeaua dumneavoastră să poată interacționa cu serverele din Internet.

Dacă dispozitivul este compatibil cu standardul NAT, o altă caracteristică pe care ar fi bine să o ofere dispozitivul este un server DHCP integrat. Dacă serverul DHCP este combinat cu dispozitivul firewall, nu mai este nevoie să configurați un alt calculator pentru acest serviciu. Deoarece unul dintre obiectivele folosirii unui dispozitiv firewall ieftin este reducerea la minimum a sarcinilor de gestionare, este logică gruparea mai multor servicii în același loc.

Raportarea și avertizarea

Deoarece un dispozitiv firewall este destinat celor care nu au prea multă experiență de lucru în rețea sau cu protocolul TCP/IP, posibilitățile de raportare și de avertizare ale dispozitivului sunt foarte importante. Dispozitivul ar trebui să fie livrat cu posibilități robuste de raportare, astfel încât, după ce vă familiarizați cu funcționarea firewall-ului, să

puteți configura rapoarte specifice. De asemenea, firewall-ul ar trebui să fie echipat cu un număr de rapoarte predefinite, care să vă permită să înțelegeți ușor datele prezentate.

De exemplu, s-ar putea să doriți un raport care să prezinte situările Web vizitate cel mai des de utilizatorii din rețea sau un raport numai cu situările Web vizitate de un anumit utilizator. Statisticile referitoare la traficul din rețea sunt importante pentru planificarea capacității, așa că rapoartele de acest tip ar trebui să conțină informații utile pentru a determina dacă legătura la Internet s-a saturat și trebuie să fie înlocuită cu un canal de capacitate mai mare. De asemenea, sunt importante rapoartele referitoare la eventualele încercări de pătrundere în rețea sau alte forme de atac.

Un dispozitiv firewall bun ar trebui să aibă posibilitatea de a vă avertiza, prin e-mail și prin pager, la apariția unei activități suspecte sau la detectarea unei posibile intruziuni. Este bine dacă dispozitivul acceptă și protocolul SNMP (Simple Network Management Protocol), dar această caracteristică este utilă mai ales într-o organizație mai mare, în care o echipă de gestionare centralizată controlează mai multe firewall-uri, eventual pentru birouri aflate la distanță.

Lucrul în rețele virtuale private (VPN – Virtual Private Networking)

Pentru orice companie ai cărei angajați trebuie să călătorească, este importantă crearea unei legături sigure de comunicație între un angajat aflat în deplasare și biroul de bază. De asemenea, o legătură sigură este importantă pentru companiile care au mai multe birouri aflate în locuri diferite. Folosind o legătură dintr-o rețea virtuală privată (VPN) puteți uita de costurile închirierii unor linii dedicate sau de tarifele pentru apelurile telefonice interurbane făcute prin modemuri. Puteți crea un canal criptat de comunicații între birouri, folosind la ambele capete același tip de dispozitiv firewall. Dacă furnizorul folosește o metodă standard pentru crearea rețelei virtuale private, în locul unei soluții brevetate, este posibil să utilizați dispozitivul firewall pentru stabilirea unei legături criptate cu un produs al unui alt furnizor.

Pentru utilizatorii mobili, firewall-ul ar trebui să fie compatibil cu un standard precum Microsoft Point-to-Point Tunneling Protocol (PPTP), deoarece sistemele de operare Windows permit utilizarea funcțiilor prevăzute de acest standard. Deoarece componentele software VPN sunt integrate în clienți de acest tip, la capătul conexiunii dinspre utilizatorul mobil nu este nevoie să folosiți un alt firewall.

Vezi și

➤ Pentru mai multe informații despre PPTP și rețelele virtuale private, vezi capitolul 10, „Rețele virtuale private (VPN) și tuneluri”, la pagina 175.

Evaluarea prețului unui dispozitiv firewall

Termenul „dispozitiv firewall” este aplicat unei game largi de produse. Există atât produse cu prețuri relativ mici – sub 1000 de dolari – cât și unele care costă mai mult de 10.000 de dolari. Unele funcționează ca produse independente, în timp ce altele pot fi folosite în

grupuri, pentru deservirea mai multor locații. Totuși, prețul pe care îl plătiți nu are întotdeauna o legătură directă cu funcționalitatea pe care o obțineți. Este important să citiți cu atenție documentația și prospectele și să puneți întrebări atunci când vreți să cumpărați un produs de acest tip.

De asemenea, verificați costurile pentru asistență tehnică și actualizări. Nici un firewall, dispozitiv sau sub altă formă, nu este un produs static, care nu trebuie schimbat niciodată. Pericolele la care este expusă rețeaua dumneavoastră în Internet evoluează și se modifică în fiecare zi. Calitatea actualizărilor software pentru un dispozitiv firewall depinde de furnizorul produsului. Ca urmare, atunci când evaluați produse similare, luați în considerare atât prețul de cumpărare, cât și costurile de asistență pe termen lung. Asigurați-vă că producătorul respectiv va rămâne pe piață o perioadă lungă, iar asistența tehnică este permanentă și include apelarea în caz de urgență.

Dispozitivele firewall îi pot induce în eroare pe unii utilizatori. Dacă vă gândiți la un firewall ca la unul dintre acele dispozitive simple pe care le conectați la rețea și uitați de ele, probabil că nu ați înțeles cât de important este un firewall și ce poate face pentru rețeaua dumneavoastră.

Rezumat

Un dispozitiv firewall este, în esență, un calculator configurat pentru executarea unei funcții specifice: să acționeze ca un zid de apărare între rețeaua dumneavoastră și Internet. Atunci când cumpărați un dispozitiv de acest tip, nu uitați să consultați documentația, pentru a determina mai întâi dacă produsul respectiv oferă caracteristicile pe care le considerați necesare pentru protecția rețelei dumneavoastră. Dacă nu înțelegeți complet terminologia folosită de producător, folosiți această carte ca referință tehnică, apălați numărul de asistență tehnică al furnizorului și puneți întrebări!

Dispozitivele firewall sunt produse la modă. Se pare că ceea ce odată era un proces complicat, a fost redus în prezent la un dispozitiv plug-and-play. În următorul capitol veți găsi subiecte referitoare la viitorul securității în Internet, precum și la locul pe care îl vor ocupa firewall-urile în acest scenariu de viitor.

Capitolul 21

Firewall-uri și mai mult decât atât

- Totul se referă la Internet
- Noi funcții
- Calculatoare casnice
- Clienți în rețele virtuale private
- IPv6: următoarea generație a protocolului IP

Totul se referă la Internet

Dacă Internetul nu ar fi existat, probabil că singurele persoane pe care le-ați fi putut auzi vorbind despre firewall-uri ar fi fost constructorii sau, poate, un administrator de securitate al unei rețele din domeniul militar. Totuși, Internetul este o realitate și milioane de oameni îl folosesc pentru nenumărate activități, de la simple mesaje de poștă electronică la tranzacții financiare complexe. Internetul este un organism aflat în dezvoltare. În fiecare zi sunt dezvoltate noi tehnologii și, o dată cu acestea, apar noi puncte vulnerabile în ceea ce privește securitatea. Din această cauză, este posibil ca în următorii ani să vedeți multe schimbări în domeniul firewall-urilor. Noi protocoale, cum ar fi IPv6, vor pune la dispoziție noi instrumente de implementare a securității și, foarte probabil, vor introduce noi pericole. Noile pericole vor crea necesitatea unor noi metode de protecție. Noi protocoale, noi pericole – acestea vor însemna noi funcționalități pentru firewall-uri.

În acest capitol vom prezenta câteva posibilități legate de dezvoltarea viitoare a firewall-urilor. De asemenea, vom discuta pe scurt despre următoarea generație a protocolului IP (IPv6), cu care vor lucra în viitor toți cei conectați la Internet.

Noi funcții

Firewall-urile curente funcționează folosind două metode de bază despre care am discutat pe larg în această carte: filtrarea pachetelor și intermedierea aplicațiilor. Pe măsură ce se dezvoltă, firewall-urile vor include noi funcții. În prezent, dacă vreți să achiziționați un

produs și comparați diferitele firewall-uri existente, veți descoperi multe „îmbunătățiri” care diferențiază produsele disponibile. Printre noile caracteristici încorporate în firewall-uri se numără:

- Noi implementări ale filtrării statice a pachetelor sau ale filtrării dinamice a pachetelor, pentru a permite o mai bună autorizare a aplicațiilor UDP printr-un firewall.
- Căutare antivirus. Această căutare se face în firewall, în loc să se aștepte ca virusul să ajungă pe calculatorul utilizatorului.
- Detectarea intruziunilor sau capacitatea de a detecta activitățile suspecte și de a răspunde la acestea. Răspunsurile ar putea include avertizarea unui administrator sau creșterea nivelului la care se face înregistrarea într-un jurnal în timpul activității suspecte.
- Tehnicile mai puternice de autentificare, cum ar fi tokenurile hardware și parolele de unică folosință, vor deveni o caracteristică foarte importantă a firewall-urilor în următorii ani.
- Posibilități de gestionare. Nu ar trebui ca administratorii să fie nevoiți să construiască seturi complicate de reguli folosind sintaxa rutelor din epoca de piatră. Interfețele grafice și programele de asistență vor deveni ceva obișnuit pentru simplificarea operațiilor de gestionare și configurare.

Vezi și

- Pentru mai multe informații despre filtrarea pachetelor, vezi capitolul 5, „Filtrarea pachetelor”, la pagina 95. Pentru mai multe informații despre intermediarii de aplicații, vezi capitolul 7, „Porți de aplicații și servere intermediar”, la pagina 132.

Furnizorii de firewall-uri vor continua să își diferențieze produsele, încercând să adauge noi caracteristici. Ar putea fi o idee bună să evaluați furnizorii înainte de a încerca să evaluați produsele. Dacă este vorba despre o tehnologie care se va schimba rapid în următorii ani (și acest lucru este adevărat în cazul firewall-urilor), probabil că vreți să faceți afaceri cu un furnizor care va mai exista peste un an. Este de dorit să faceți afaceri cu un furnizor care va continua să își dezvolte produsele.

Integrarea firewall-urilor

Este ușor să vă gândiți la un firewall ca la un punct unic de trecere, care poate fi folosit pentru monitorizarea traficului între rețeaua dumneavoastră și Internet. În practică, multe organizații mari instalează firewall-uri multiple. Acestea pot fi folosite pentru asigurarea securității conexiunilor multiple la Internet sau a conexiunilor dintre departamente ori cu clienții sau alți parteneri de afaceri. Gestionarea firewall-urilor multiple într-o asemenea situație poate fi o sarcină cu adevărat obositoare.

Noile produse pentru firewall-uri ar trebui să fie configurate astfel încât să poată fi gestionate centralizat, de preferat prin folosirea unei interfețe grafice ușor de înțeles. Dezvoltarea interfețelor standardizate de programare a aplicațiilor (API – Application Programming Interface) care funcționează cu protocoale și standarde de securitate recunoscute va contribui la simplificarea integrării produselor provenite de la diferiți furnizori. Prin folosirea standardelor, va fi posibilă gestionarea produselor pentru firewall-uri la fel ca în cazul multor alte dispozitive de rețea, prin SNMP, RMON sau, eventual, o extensie a acestora dezvoltată special pentru firewall-uri.

¹ Termenul *firewall* (*parașoc*) este împrumutat din domeniul construcțiilor, unde reprezintă un zid (perete) de protecție, care, de exemplu, apără de flăcări părțile mai expuse ale unui cazan cu aburi, sau, într-o clădire, împiedică extinderea focului în cazul unui incendiu (n. trad.)

Testarea firewall-urilor

Una dintre cele mai dificile sarcini pe care trebuie să le îndeplinească un administrator care tocmai a instalat un firewall este să determine cât de bine funcționează acesta. În timpul instalării, trebuie să luați diferite decizii privind modul de configurare a firewall-ului. Seturile complexe de reguli, în special pentru un ruter, pot fi dificil de înțeles și pot avea ca rezultat breșe de securitate. Dacă nu aveți o metodă de testare a firewall-ului, cum puteți ști care este nivelul de protecție obținut?

O modalitate este să așteptați să se întâmple ceva și apoi să rezolvați problema. Desigur, aceasta nu este modalitatea ideală de a testa un firewall. În schimb, furnizorii trebuie să pună la dispoziție aplicații care pot fi folosite din ambele părți ale firewall-ului pentru verificarea breșelor de securitate și prezentarea datelor într-un format pe care administratorul să îl înțeleagă cu ușurință. Deși este posibil ca un administrator de rețea experimentat, care cunoaște sistemul de operare UNIX, să folosească utilitare precum COPS sau SATAN pentru verificarea rețelei, mulți administratori nu au pregătirea necesară pentru utilizarea acestor instrumente. Furnizorii care pot asigura programe de testare complete pentru produsele proprii vor găsi mulți clienți interesați.

Vezi și

- *Puteți obține produsele COPS și SATAN și le puteți folosi pentru a evalua profilul de securitate al rețelei dumneavoastră. Aceste utilitare, împreună cu altele, sunt prezentate în anexa B, „Alte instrumente de securitate pe care le puteți folosi”; la pagina 364.*

Calculatoare casnice

Până de curând, produselor de tip firewall destinate uzului casnic li s-a acordat foarte puțină atenție. Acasă, principala problemă a unui utilizator era posibila descărcare a unui virus sau a unui cal troian. Pentru protecția împotriva virușilor s-a dezvoltat o întreagă industrie. Deoarece majoritatea conexiunilor casnice la Internet se bazează pe linii telefonice comutate, cei mai mulți dintre acești utilizatori nu rămân în Internet un timp suficient pentru a permite unui hacker să pătrundă în sistem.

Totuși, situația se schimbă în urma apariției și instalării liniilor digitale (Digital Subscriber Line – DSL). Modemurile pentru cablu sunt folosite din ce în ce mai mult ca modalitate de conectare la Internet. În comparație cu accesul printr-un modem pe linie comutată, acestea prezintă o diferență importantă. Atunci când vă deconectați de la un modem pe linie comutată, vă deconectați de la Internet. În cazul folosirii unui modem pentru cablu, deschiderea conexiunii nu se face printr-un apel telefonic. Sunteți permanent on-line. Chiar dacă nu stați la calculator, răsfoind paginile din Internet, dar acesta este pornit și încărcat, este posibil ca un intrus să se infiltreze pe calculatorul dumneavoastră.

Câteva dintre cele mai recente instrumente pentru hackeri, cum ar fi instrumentele de atac prin blocarea unui serviciu¹, folosesc zeci sau sute de calculatoare ai căror proprietari nu

¹ Numit și atac DoS (denial of service), atac prin refuzarea unui serviciu sau atac prin interzicerea unui serviciu (n. trad.)

bănuiesc nimic, pentru a lansa un atac asupra unei ținte. Hackerul caută gazde aflate on-line care folosesc măsuri minime de securitate. Dacă vă gândiți puțin, calculatoarele casnice sunt ideale din acest punct de vedere.

Vezi și

- *Pentru mai multe informații despre instrumentele de atac prin blocarea unui serviciu, cum ar fi Tribe Flood și Stacheldrabt, vezi secțiunea „Atacuri de tip interzicerea serviciului” din capitolul 3, „Securitate și Internet”, la pagina 63.*

În prezent sunt în curs de apariție mai multe produse destinate utilizatorilor casnici de calculatoare. Vă puteți aștepta ca în viitor să vedeți un număr mai mare de asemenea produse. Până atunci, dacă sunteți un utilizator DSL, gândiți-vă că ar trebui să opriți calculatorul și să îl deconectați de la cablu atunci când nu îl folosiți!

Clienți în rețele virtuale private

O parte dintre tehnologiile pe care de obicei le asociați cu firewall-urile sunt transferate în sistemul de operare client. De exemplu, firewall-urile sunt folosite în mod obișnuit pentru crearea unei rețele virtuale private (VPN) între două rețele, astfel încât clienții și serverele din cele două rețele să poată comunica în siguranță prin intermediul unei rețele nesigure – cum ar fi Internetul. Microsoft a dezvoltat produsele VPN pentru a fi folosite în Windows NT 4.0 împreună cu serviciul de acces de la distanță (RAS). În Windows 2000, Microsoft a extins posibilitățile produselor VPN prin încorporarea unor noi protocoale, cum ar fi IPSec și L2PT, pe lângă implementarea originală, bazată pe PPTP.

Vezi și

- *Pentru mai multe informații despre IPSEC, PPTP și L2PT, vezi capitolul 10, „Rețele virtuale private (VPN) și tuneluri”, la pagina 175.*

Firewall-urile care folosesc pentru rețelele VPN o tehnologie brevetată pot stabili un canal sigur numai cu alte dispozitive care folosesc aceeași tehnologie. Firewall-urile mai noi și cele pe care este de așteptat să le vedeți în următorii ani vor folosi protocoale standard. Ca urmare, veți putea să creați rețele VPN între firewall-uri provenite de la furnizori diferiți. Deoarece vor fi folosite protocoale standard, vă puteți aștepta și la alte dezvoltări la nivelul clientului, ceea ce va permite gazdelor individuale să creeze rețele VPN între ele și firewall, sau poate chiar între ele și alte gazde, ocolind complet firewall-ul.

IPv6: următoarea generație a protocolului IP

Forumul IPv6 și IPv6.org

Există câteva situri Web dedicate protocolului IP din următoarea generație. La adresa www.ipv6.org veți găsi un sit Web care conține legături către lista de întrebări puse frecvent cu privire la IPv6, specificații, o listă de poșta electronică și alte informații.

IPv6 Forum este un consorțiu de furnizori și alte companii care promovează adoptarea și utilizarea protocolului IPv6. Puteți vizita situl Web al acestui forum la adresa www.ipv6forum.com.

Dintre toate tehnologiile pe care vă puteți aștepta să le folosiți în următorii ani, una va avea un impact puternic asupra construcției firewall-urilor. Aceasta este următoarea generație a protocolului IP.

Versiunea curentă a protocolului IP (IPv4) are aproape 20 de ani și începe să-și arate vârsta. Spațiul total de adrese pe care îl asigură IPv4 este pe cale de a se epuiza rapid. Hackerii caută continuu slăbiciuni ale protocolului și ale serviciilor care îl folosesc. Serviciile mai noi ar putea fi construite mai bine dacă protocolul, care stă la baza Internetului, ar fi puțin mai robust. Din toate aceste motive, la care se adaugă și altele, ar trebui să fie evident că următoarea generație a protocolului IP, versiunea 6 (IPv6), ține de viitorul apropiat. Primele eforturi de elaborare a protocolului IPv6 au fost făcute la începutul anilor '90, iar prima propunere a standardului a fost aprobată în noiembrie 1994, prin documentul Request For Comments (RFC) 1752, „Recomandări pentru următoarea generație a protocolului IP”¹.

Trecerea la protocolul IPv6 nu va fi bruscă, ci se va face printr-un proces evolutiv. IPv6 poate interopera cu IPv4, așa că, probabil, va fi o perioadă de coexistență pașnică a celor două versiuni după introducerea protocolului IPv6.

Antetul IPv6

Noul antet IP are o lungime fixă de 40 de octeți. Prin folosirea unui antet cu lungime fixă, este posibilă crearea unor dispozitive de rețea care pot prelucra pachetele mult mai rapid decât în cazul manipulării unor anteturi cu lungime variabilă. Noul antet, așa cum puteți vedea în figura 21.1, conține mai puține câmpuri decât antetul IPv4.

FIGURA 21.1

Antetul IPv6 are o lungime fixă de 40 de octeți.

Versiune (Version)	Clasă de trafic (Traffic Class)	Etichetă de flux (Flow Label)		
Dimensiunea conținutului util (Payload Length)		Următorul antet (Next Header)	Limită de salturi (Hop Limit)	
Adresa sursei (Source Address)				
Adresa destinației (Destination Address)				

Exceptând numărul mai mic de câmpuri, cea mai evidentă modificare a antetului IPv6 o reprezintă câmpurile mai mari pentru adrese. Atât pentru sursă, cât și pentru destinație, sunt folosite câmpuri de câte 128 de biți. Această îmbunătățire ar trebui să pună la dispoziție în Internet destule adrese pentru identificarea unică a fiecărui grăunte de nisip de pe planetă, ceea ce ar trebui să fie suficient, măcar pentru câțiva ani de-acum încolo.

¹ RFC 1752, „The Recommendation for the IP Next Generation Protocol” (n. trad.)

Interoperarea protocoalelor IPv4 și IPv6

Cum pot lucra împreună noduri IPv4 și IPv6 aflate în aceeași rețea? În prezent există două propuneri. Prima constă în crearea noilor sisteme IPv6 astfel încât acestea să folosească două stive de protocoale diferite, una pentru IPv4 și una pentru IPv6, în funcție de nodul cu care comunică. A doua metodă propune încapsularea pachetelor IPv6 în pachete IPv4 atunci când datele sunt transmise între două mașini IPv6 pe o rută care conține mașini IPv4.

Vezi și

➤ *Antetul IPv4 și câmpurile acestuia sunt prezentate în detaliu în capitolul 2, „Introducere în suita de protocoale TCP/IP”, la pagina 26.*

Câmpurile incluse în antetul IPv4 care nu vor mai fi folosite în antetul IPv6 sunt:

- Câmpurile legate de fragmentare, cum ar fi câmpurile Fragment Offset și Identification Field, precum și indicatorii Don't Fragment și More Fragments
- Câmpul pentru suma de verificare (Checksum)
- Câmpul de opțiuni

Pentru a crește viteza de prelucrare, în versiunea IPv6 s-a renunțat la fragmentarea pachetelor. Dacă un pachet este prea mare pentru ca un ruter să îl retransmită printr-o legătură de rețea, pachetul nu este împărțit în pachete mai mici și apoi reasamblat la destinație. Pachetul va fi abandonat și către expeditor va fi trimis un nou mesaj ICMP („Packet Too Big” – „Pachet prea mare”). Stația emițătoare poate apoi să creeze pachete mai mici în vederea transmisiei.

Tot cu intenția de a crește viteza de prelucrare a pachetelor, IPv6 nu are în antet un câmp pentru suma de verificare. Pentru fiecare ruter pe care trebuie să îl traverseze pachetul IPv6, acest câmp trebuie să fie recalculat, deoarece câmpul TTL este decrementat la fiecare salt. Deoarece atât stratul legăturii de date, aflat sub IP, cât și unele protocoale de pe nivelurile superioare, cum ar fi TCP și UDP, realizează funcția de calculare a sumei de verificare, este de așteptat ca eliminarea acesteia din antetul IP să nu creeze nici o problemă.

Situația este diferită în cazul câmpului de opțiuni. Deși acest câmp cu lungime variabilă a fost eliminat din antetul IP, astfel încât antetul să poată avea o lungime fixă, nu înseamnă că s-a renunțat complet la prelucrarea opțiunilor. Dacă în pachet sunt folosite opțiuni, câmpul Next Header, care în mod normal indică un alt protocol, cum ar fi TCP sau UDP, poate fi folosit pentru specificarea opțiunilor. În această situație, informațiile despre opțiuni sunt incluse în secțiunea de date utile a pachetului și sunt identificate de câmpul Next Header. Și în acest caz, eliminând din antet prelucrarea opțiunilor și permițând folosirea anteturilor cu lungime fixă, prelucrarea pachetelor IP poate fi făcută mult mai repede.

Noul protocol ICMP

Protocolul ICMP (Internet Control Message Protocol) este folosit de IP pentru diferite funcții. Cea mai cunoscută utilizare a acestuia este utilitarul PING, care folosește mesaje de ecou pentru a determina dacă o gazdă aflată la distanță în rețea este accesibilă. Așa cum protocolul IP va suferi o transformare, și protocolul ICMP va fi îmbunătățit pentru a face față schimbărilor. În afara modificărilor determinate de IPv6, ICMP va include și funcționalitatea protocolului IGMP (Internet Group Management Protocol). În documentul RFC 2463, „Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)”, puteți găsi o prezentare a modificărilor efectuate în ICMP.

Vezi și

- Pentru mai multe informații despre Internet Control Message Protocol (ICMP), vezi secțiunea „Protocolul ICMP (Internet Control Message Protocol)” din capitolul 2, „Introducere în suita de protocoale TCP/IP”, la pagina 33.

Câmpurile din noul antet IPv6 sunt:

- **Versiune (Version)** – Ca și în versiunea IPv4, acest câmp de patru biți este folosit pentru a specifica versiunea protocolului IP. Pentru IPv6, valoarea acestui câmp va fi întotdeauna 6.
- **Clasă de trafic (Traffic Class)** – Funcția acestui câmp de opt biți este asemănătoare cu cea a câmpului TOS (Type Of Service) din antetul IPv4, deși modalitatea de implementare nu este încă clarificată.
- **Etichetă de flux (Flow Label)** – Acest câmp va fi folosit pentru identificarea diferitelor fluxuri de trafic¹ pentru care expeditorul solicită un tratament special. Definiția exactă a unui flux nu este încă stabilită complet. Ar putea fi trafic provenit de la un utilizator care plătește mai mult pentru un anumit serviciu sau trafic folosit pentru programe audio ori video.
- **Dimensiunea conținutului util (Payload Length)** – Această valoare este un câmp de 16 biți, specificând numărul de octeți ce urmează după antet.
- **Următorul antet (Next Header)** – Acest câmp folosește aceleași numere de protocoale ca și IPv4 și este utilizat pentru specificarea protocolului de nivel superior către care va fi livrat pachetul în vederea prelucrării ulterioare.
- **Limită de salturi (Hop Limit)** – Numărul maxim de salturi permise pentru fiecare pachet. Fiecare ruter decrementează această valoare cu o unitate. Dacă valoarea câmpului ajunge la zero, pachetul este abandonat.
- **Adresa sursei (Source Address)** – Un câmp de 128 de biți, identificând sursa pachetului.
- **Adresa destinației (Destination Address)** – Un câmp de 128 de biți, identificând destinația pachetului.

Anteturi de extensie

În antetul cu lungime fixă de 40 de octeți, câmpul Next Header este folosit pentru a indica tipul antetului care va fi găsit la începutul câmpului de date din pachet. Nu uitați că, de obicei, IP încapsulează un protocol de nivel superior, cum ar fi TCP sau UDP, iar aceste protocoale au propriile informații de antet. Prin folosirea unui antet IP cu lungime fixă, poate fi mărită viteza de prelucrare a pachetelor de către rutere și alte gazde din rețea. Totuși, deoarece din pachet au fost omise unele câmpuri, este necesară o altă metodă pentru a asigura funcționalitatea pierdută.

Din acest motiv, există câteva tipuri de *anteturi de extensie*, care pot apărea la începutul porțiunii de date a pachetului IP. Câmpul Next Header va identifica un antet de extensie ca și cum acesta ar fi următorul antet pentru protocolul de nivel superior. Principalele anteturi de extensie care pot fi folosite sunt:

- Opțiuni salt-cu-salt (Hop-by-Hop Options)
- Fragmentare (Fragmentation)

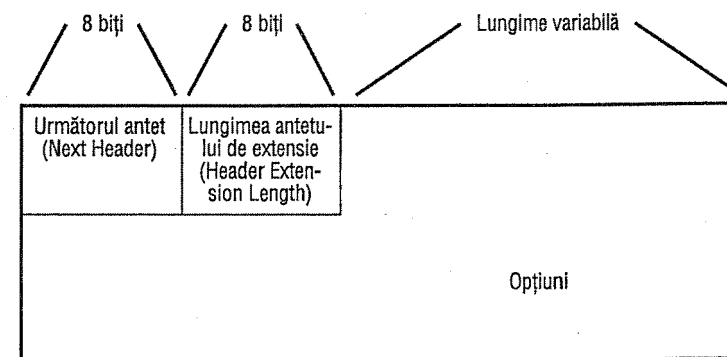
¹ În original, *slow or stream of traffic* (n. trad.)

- Rutare (Routing)
- Autentificare (Authentication)
- Încapsulare de securitate (Security Encapsulation)
- Încapsulare a conținutului util de securitate (Encapsulating Security Payload)
- Opțiuni pentru destinație

Primul tip de antet de extensie, opțiuni salt-cu-salt, este identificat prin stocarea valorii 0 în câmpul Next Header. Acest antet este folosit pentru informații pe care trebuie să le examineze fiecare sistem aflat pe traseul parcurs de pachet. Singura opțiune definită în acest moment este cea care permite transmiterea pachetelor cu conținut foarte mare (Jumbo Payload), adică pachete IP mai mari de 65.535 de octeți. Dacă vă uitați la formatul antetului de extensie pentru opțiuni salt-cu-salt (figura 21.2), veți vedea că acesta conține un câmp pentru următorul antet (Next Header), la fel ca și antetul IPv6. În acest fel este permisă folosirea mai multor anteturi de extensie, fiecare indicând următorul antet.

FIGURA 21.2

Formatul antetului de extensie pentru opțiuni salt-cu-salt.



Câte adrese IPv4?

Teoretic, folosind mecanismul de adresare IPv4, este posibil să fie adresate peste 16 milioane de rețele și peste 4 miliarde de gazde individuale. Deoarece pe planetă există deja peste 6 miliarde de oameni și sunt alocate din ce în ce mai multe adrese, ne putem da seama ușor că rezerva de adrese se va epuiza în viitorul apropiat. Nu uitați că o persoană nu trebuie neapărat să aibă o singură adresă. Pe măsură ce tot mai multe dispozitive, cum ar fi telefoanele celulare și PDA (asistenți digitali personali), înglobează facilități pentru Internet, va deveni ceva obișnuit ca o persoană să folosească mai multe adrese.

Antetul de extensie pentru fragmentare, identificat de valoarea 44 în câmpul Next Header, este folosit atunci când sursa pachetului determină că mesajul trebuie să fie fragmentat în vederea transmiterii prin rețea. Nu uitați că în IPv6 nu este prevăzută fragmentarea pachetului pe durata rutării în rețea. Această funcție a fost omisă pentru creșterea vitezei de prelucrare a pachetelor IP. Orice operație de fragmentare a mesajului se face acum la sursa pachetului, iar antetul de extensie este folosit pentru stocarea informațiilor despre acest proces, astfel încât gazda de la capătul de recepție să poată reasambla corect pachetul.

Antetul de extensie pentru opțiunile de rutare (valoarea 43 în câmpul Next Header) funcționează asemănător cu rutarea la sursă din IPv4. Acest antet este folosit pentru a specifica unul sau mai multe noduri pe care un pachet ar trebui să le viziteze în timpul traversării rețelei.

Antetul de extensie cu opțiuni pentru destinație (valoarea 60 în câmpul Next Header) este folosit pentru stocarea unor informații pe care trebuie să le examineze numai nodul destinație.

Vezi și

- *Anteturile de extensie legate de securitate și autentificare sunt definite de alte documente RFC. De exemplu, Authentication Header și Encapsulating Security Payload sunt definite în documentele RFC 2402 și 2406. Pentru mai multe informații despre acestea și despre alte protocoale legate de securitate, vezi capitolul 10, „Rețele virtuale private (VPN) și tuneluri”, la pagina 175.*

O valoare 59 în câmpul Next Header arată că nu mai există alte anteturi care trebuie să fie examinate. Dacă valoarea Payload Length indică faptul că există octeți suplimentari ce conțin informații de antet, acești octeți vor fi ignorați după găsirea unui antet care conține valoarea 59 în câmpul Next Header.

Adresarea în IPv6

Așa cum probabil vă imaginați, în urma trecerii de la 32 la 128 de biți, spațiul de adrese din IPv6 este mult mai mare decât în IPv4.

IPv6 va avea trei tipuri de adrese de bază:

- **Unicast** (adresă unică) – O adresă care identifică în mod unic o anumită interfață de rețea.
- **Anycast** (orice adresă) – O adresă folosită de mai multe interfețe de rețea. Un pachet rutat către o adresă de acest tip va fi transmis către cea mai apropiată interfață cu această adresă (determinată de protocolul de rutare folosit).
- **Multicast** (adresă de difuzare pe grupuri) – Și adresele de acest tip identifică mai multe interfețe de rețea cu aceeași adresă. Totuși, spre deosebire de adresele anycast, un pachet transmis către o adresă de difuzare pe grupuri este rutat către toate interfețele cu adresa respectivă.

Deși o adresă unicast identifică în mod unic o interfață de rețea, aceeași interfață poate avea mai multe adrese unicast. Adresele de difuzare (broadcast) au dispărut. Funcționalitatea acestora a fost încorporată în adresele de tip multicast.

Spre deosebire de IPv4, adresele IPv6 nu au clase. Aceasta înseamnă că nu există identificatoare pentru adrese de clase A, B sau C. De asemenea, adresele reale sunt puțin mai complicate decât în formatul IPv4. Pentru mai multe detalii, ar trebui să citiți documentul RFC (Request For Comments) 2373, „Arhitectura de adresare a protocolului IP, Versiunea 6”¹.

Tranziția la IPv6

Următoarea generație a protocolului IP este în curs de dezvoltare de mai mulți ani. Epuizarea spațiului de adrese IPv4 a fost amânată câțiva ani prin introducerea unor tehnologii precum Network Address Translation (Traducerea adreselor de rețea). Totuși,

¹ RFC 2373, „IP Version 6 Addressing Architecture” (n. trad.)

avantajele așteptate de la IPv6 nu se rezumă la o simplă extindere a spațiului de adrese, așa că adoptarea acestui protocol ține de viitorul apropiat.

Revenind la o idee menționată anterior, se așteaptă ca trecerea la IPv6 să nu se facă brusc. Tranziția va fi graduală, cu dispozitive de rețea proiectate să lucreze atât cu IPv4, cât și cu IPv6. Documentul RFC 1993, „Mecanismul de tranziție pentru gazdele și ruterele IPv6”¹, discută două metode luate în considerare. Prima metodă folosește dispozitive de rețea cu stive duale de protocoale, care pot răspunde atât la pachete IPv4, cât și la pachete IPv6. A doua metodă asigură transferarea prin tunel a datagramelor IPv6 în interiorul unui pachet IPv4.

Rezumat

Cu zece ani în urmă, dacă ați fi menționat crearea unui firewall pentru rețeaua dumneavoastră, puțini oameni ar fi știut despre ce vorbiți. Desigur, dacă ați fi spus acum zece ani că urmează să vă conectați la Internet, nu mulți ar fi știut despre ce este vorba.

În prezent, Internetul se răpândește rapid și în curând va fi omniprezent, ca și rețeaua telefonică. Posibilitățile de încorporare a tehnologiilor de rețea în tot felul de dispozitive folosite în mod uzual vor genera în viitorul apropiat noi tehnologii și domenii industriale. Pe măsură ce tehnologia progresează, vor fi descoperite și noi vicii de securitate. Pentru a le face față, va trebui să se schimbe și tehnologia firewall-urilor. Pe măsură ce vor fi implementate IPv6 și alte protocoale, vor fi introduse și noi tehnici de securitate. Deoarece securitatea devine o problemă din ce în ce mai importantă pentru cei interesați, produsele pentru firewall-uri nu vor mai fi ceva atât de neobișnuit în mediile de calcul casnice.

¹ RFC 1993, „Transition Mechanism for IPv6 Hosts and Routers” (n. trad.)

Partea a IV-a

Anexe

Anexa A • Porturi uzuale TCP și UDP	317
Anexa B • Alte instrumente de securitate pe care le puteți folosi	364
Anexa C • Resurse suplimentare	372

Anexa A

Porturi uzuale TCP și UDP

Înțelegerea porturilor

Calculatoarele din Internet folosesc suita de protocoale de rețea TCP/IP pentru a comunica între ele. Ca urmare, fiecare calculator trebuie să aibă propria adresă IP pentru a fi identificat în mod unic în Internet. Dacă nu ar fi nevoie decât de un canal de comunicație între două calculatoare, adresa IP ar fi singura informație necesară pentru a permite aplicațiilor de pe calculatoare să comunice între ele. Dar ce se întâmplă atunci când mai multe aplicații de pe un calculator trebuie să comunice cu aplicații de pe alte calculatoare? Evident, trebuie să existe un alt mecanism care să poată fi folosit pentru a identifica destinația unui pachet de rețea.

Pentru această identificare suplimentară sunt folosite numerele de porturi. Adresa IP destinație dintr-un pachet precizează calculatorul de la distanță către care este transmis pachetul. Numărul de port, care este stocat tot în antetul pachetului, îi precizează calculatorului destinația *aplicația* căreia îi este destinat pachetul. Pentru a face o analogie, adresa IP este asemănătoare cu adresa poștală a unei clădiri. Folosind adresa poștală, puteți face ca o scrisoare să ajungă la clădirea corectă. Dacă doriți ca scrisoarea să ajungă rapid la Bob Smith, aflat la etajul patru, trebuie să includeți în adresă și numărul biroului sau al apartamentului. Acest număr este similar cu un număr de port.

Numerele de porturi au valori de la 0 la 65535. Porturile de la 0 la 1023 sunt numite *porturi recunoscute*¹ și sunt alocate de organizația Internet Assigned Numbers Authority (IANA). Utilizarea acestor porturi a fost definită în mai multe documente Request For Comments (cel mai recent fiind RFC 1700) și nu se schimbă foarte des. Tabelul A.1 prezintă o listă a acestor porturi, împreună cu o scurtă descriere a modului de folosire.

Deoarece, pentru un sistem dat, porturile recunoscute sunt accesibile de obicei proceselor privilegiate sau utilizatorilor privilegiați, este important ca atunci când configurați un firewall să înțelegeți pentru ce este folosit fiecare port, astfel încât să puteți decide ce porturi trebuie să blocați. În general, utilitarul Telnet folosește portul 23. Totuși, rețineți că unele versiuni mai sigure ale unui anumit utilitar pot folosi alte porturi decât versiunea obișnuită a aceluiași utilitar. Documentația furnizată împreună cu o asemenea aplicație ar trebui să vă pună la dispoziție și aceste informații.

Porturile cu numere de la 1024 la 65535 nu sunt guvernate de IANA. Aceste porturi sunt numite *porturi înregistrate* și pot fi folosite de aproape orice proces de utilizator din sistem.

În cele mai multe cazuri, protocoalele UDP (User Datagram Protocol) și TCP (Transmission Control Protocol) utilizează același număr pentru un anumit port. Totuși, acest

¹ În original, *well-known ports*. Numite și *porturi general cunoscute* (n. trad.)

lucru nu este obligatoriu, așa că atunci când folosiți acest tabel, nu uitați să verificați protocolul pentru fiecare port a cărui utilizare o căutați.

Tabelul A.1 Numere de porturi recunoscute TCP și UDP

Serviciu	Număr de port	Protocol	Descriere
	0	tcp	Rezervat
	0	udp	Rezervat
tcpmux	1	tcp	TCP Port Service Multiplexer
tcpmux	1	udp	TCP Port Service Multiplexer
compressnet	2	tcp	Management Utility
compressnet	2	udp	Management Utility
compressnet	3	tcp	Compression Process
compressnet	3	udp	Compression Process
rje	5	tcp	Remote Job Entry
rje	5	udp	Remote Job Entry
echo	7	tcp	Echo
echo	7	udp	Echo
discard	9	tcp	Discard
discard	9	udp	Discard
systat	11	tcp	Active Users
systat	11	udp	Active Users
daytime	13	tcp	Daytime (RFC 867)
daytime	13	udp	Daytime (RFC 867)
qotd	17	tcp	Quote of the Day
qotd	17	udp	Quote of the Day
misp	18	tcp	Message Send Protocol
misp	18	udp	Message Send Protocol
chargen	19	tcp	Character Generator
chargen	19	udp	Character Generator
ftp-data	20	tcp	File Transfer (Date prestabilite)
ftp-data	20	udp	File Transfer (Date prestabilite)

Serviciu	Număr de port	Protocol	Descriere
ftp	21	tcp	File Transfer (Control)
ftp	21	udp	File Transfer (Control)
ssh	22	tcp	SSH Remote Login Protocol
ssh	22	udp	SSH Remote Login Protocol
telnet	23	tcp	Telnet
telnet	23	udp	Telnet
	24	tcp	Orice sistem privat de poștă electronică
	24	udp	Orice sistem privat de poștă electronică
smtp	25	tcp	Simple Mail Transfer
smtp	25	udp	Simple Mail Transfer
nsw-fe	27	tcp	NSW User System FE
nsw-fe	27	udp	NSW User System FE
msg-icp	29	tcp	MSG ICP
msg-icp	29	udp	MSG ICP
msg-auth	31	tcp	MSG Authentication
msg-auth	31	udp	MSG Authentication
dsp	33	tcp	Display Support Protocol
dsp	33	udp	Display Support Protocol
	35	tcp	Orice server de tipărire privat
	35	udp	Orice server de tipărire privat
time	37	tcp	Time
time	37	udp	Time
rap	38	tcp	Route Access Protocol
rap	38	udp	Route Access Protocol
rlp	39	tcp	Resource Location Protocol
rlp	39	udp	Resource Location Protocol
graphics	41	tcp	Graphics
graphics	41	udp	Graphics
name	42	tcp	Host Name Server

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
name	42	udp	Host Name Server
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	Who Is
nicname	43	udp	Who Is
mpm-flags	44	tcp	MPM FLAGS Protocol
mpm-flags	44	udp	MPM FLAGS Protocol
mpm	45	tcp	Message Processing Module [recv]
mpm	45	udp	Message Processing Module [recv]
mpm-snd	46	tcp	MPM [default send]
mpm-snd	46	udp	MPM [default send]
ni-ftp	47	tcp	NI FTP
ni-ftp	47	udp	NI FTP
auditd	48	tcp	Digital Audit Daemon
auditd	48	udp	Digital Audit Daemon
tacacs	49	tcp	Login Host Protocol (TACACS)
tacacs	49	udp	Login Host Protocol (TACACS)
re-mail-ck	50	tcp	Remote Mail Checking Protocol
re-mail-ck	50	udp	Remote Mail Checking Protocol
la-maint	51	tcp	IMP Logical Address Maintenance
la-maint	51	udp	IMP Logical Address Maintenance
xns-time	52	tcp	XNS Time Protocol
xns-time	52	udp	XNS Time Protocol
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
xns-ch	54	tcp	XNS Clearinghouse
xns-ch	54	udp	XNS Clearinghouse
isi-gl	55	tcp	ISI Graphics Language

Serviciu	Număr de port	Protocol	Descriere
isi-gl	55	udp	ISI Graphics Language
xns-auth	56	tcp	XNS Authentication
xns-auth	56	udp	XNS Authentication
	57	tcp	Orice acces de terminal privat
	57	udp	Orice acces de terminal privat
xns-mail	58	tcp	XNS Mail
xns-mail	58	udp	XNS Mail
	59	tcp	Orice serviciu de fișiere privat
	59	udp	Orice serviciu de fișiere privat
	60	tcp	Nealocat
	60	udp	Nealocat
ni-mail	61	tcp	NI MAIL
ni-mail	61	udp	NI MAIL
acas	62	tcp	ACA Services
acas	62	udp	ACA Services
whois++	63	tcp	whois++
whois++	63	udp	whois++
covia	64	tcp	Communications Integrator (CI)
covia	64	udp	Communications Integrator (CI)
tacacs-ds	65	tcp	TACACS-Database Service
tacacs-ds	65	udp	TACACS-Database Service
sql*net	66	tcp	Oracle SQL*NET
sql*net	66	udp	Oracle SQL*NET
bootps	67	tcp	Bootstrap Protocol Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	tcp	Bootstrap Protocol Client
bootpc	68	udp	Bootstrap Protocol Client
tftp	69	tcp	Trivial File Transfer
tftp	69	udp	Trivial File Transfer

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
gopher	70	tcp	Gopher
gopher	70	udp	Gopher
netrjs-1	71	tcp	Remote Job Service
netrjs-1	71	udp	Remote Job Service
netrjs-2	72	tcp	Remote Job Service
netrjs-2	72	udp	Remote Job Service
netrjs-3	73	tcp	Remote Job Service
netrjs-3	73	udp	Remote Job Service
netrjs-4	74	tcp	Remote Job Service
netrjs-4	74	udp	Remote Job Service
	75	tcp	Orice serviciu de apel telefonic privat
	75	udp	Orice serviciu de apel telefonic privat
deos	76	tcp	Distributed External Object Store
deos	76	udp	Distributed External Object Store
	77	tcp	Orice serviciu privat RJE
	77	udp	Orice serviciu privat RJE
vettcp	78	tcp	vettcp
vettcp	78	udp	vettcp
finger	79	tcp	Finger
finger	79	udp	Finger
http	80	tcp	World Wide Web HTTP
http	80	udp	World Wide Web HTTP
www	80	tcp	World Wide Web HTTP
www	80	udp	World Wide Web HTTP
www-http	80	tcp	World Wide Web HTTP
www-http	80	udp	World Wide Web HTTP
hosts2-ns	81	tcp	HOSTS2 Name Server
hosts2-ns	81	udp	HOSTS2 Name Server

Serviciu	Număr de port	Protocol	Descriere
xfer	82	tcp	XFER Utility
xfer	82	udp	XFER Utility
mit-ml-dev	83	tcp	MIT ML Device
mit-ml-dev	83	udp	MIT ML Device
ctf	84	tcp	Common Trace Facility
ctf	84	udp	Common Trace Facility
mit-ml-dev	85	tcp	MIT ML Device
mit-ml-dev	85	udp	MIT ML Device
mfcobol	86	tcp	Micro Focus Cobol
mfcobol	86	udp	Micro Focus Cobol
	87	tcp	Orice legătură privată de tip terminal
	87	udp	Orice legătură privată de tip terminal
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
su-mit-tg	89	tcp	SUMIT Telnet Gateway
su-mit-tg	89	udp	SUMIT Telnet Gateway
dnsix	90	tcp	DNSIX Securit Attribute Token Map
dnsix	90	udp	DNSIX Securit Attribute Token Map
mit-dov	91	tcp	MIT Dover Spooler
mit-dov	91	udp	MIT Dover Spooler
npp	92	tcp	Network Printing Protocol
npp	92	udp	Network Printing Protocol
dcp	93	tcp	Device Control Protocol
dcp	93	udp	Device Control Protocol
objcall	94	tcp	Tivoli Object Dispatcher
objcall	94	udp	Tivoli Object Dispatcher
supdup	95	tcp	SUPDUP
supdup	95	udp	SUPDUP
dixie	96	tcp	DIXIE Protocol Specification

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
dixie	96	udp	DIXIE Protocol Specification
swift-rvf	97	tcp	Swift Remote Virtual File Protocol
swift-rvf	97	udp	Swift Remote Virtual File Protocol
tacnews	98	tcp	TAC News
tacnews	98	udp	TAC News
metagram	99	tcp	Metagram Relay
metagram	99	udp	Metagram Relay
newacct	100	tcp	[utilizare neautorizată]
hostname	101	tcp	NIC Host Name Server
hostname	101	udp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
iso-tsap	102	udp	ISO-TSAP Class 0
gppitnp	103	tcp	Genesis Point-to-Point Trans Net
gppitnp	103	udp	Genesis Point-to-Point Trans Net
acr-nema	104	tcp	ACR-NEMA Digital Imag. & Comm. 300
acr-nema	104	udp	ACR-NEMA Digital Imag. & Comm. 300
cso	105	tcp	CCSO Name Server Protocol
cso	105	udp	CCSO Name Server Protocol
csnet-ns	105	tcp	Mailbox Name Nameserver
csnet-ns	105	udp	Mailbox Name Nameserver
3com-tsmux	106	tcp	3COM-TSMUX
3com-tsmux	106	udp	3COM-TSMUX
rtelnet	107	tcp	Remote Telnet Service
rtelnet	107	udp	Remote Telnet Service
snagas	108	tcp	SNA Gateway Access Server
snagas	108	udp	SNA Gateway Access Server
pop2	109	tcp	Post Office Protocol-Version 2
pop2	109	udp	Post Office Protocol-Version 2

Serviciu	Număr de port	Protocol	Descriere
pop3	110	tcp	Post Office Protocol-Version 3
pop3	110	udp	Post Office Protocol-Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
mcidas	112	tcp	McIDAS Data Transmission Protocol
mcidas	112	udp	McIDAS Data Transmission Protocol
ident	113	tcp	
auth	113	tcp	Authentication Service
auth	113	udp	Authentication Service
audionews	114	tcp	Audio News Multicast
audionews	114	udp	Audio News Multicast
sftp	115	tcp	Simple File Transfer Protocol
sftp	115	udp	Simple File Transfer Protocol
ansanotify	116	tcp	ANSA REX Notify
ansanotify	116	udp	ANSA REX Notify
uucp-path	117	tcp	UUCP Path Service
uucp-path	117	udp	UUCP Path Service
sqlserv	118	tcp	SQL Services
sqlserv	118	udp	SQL Services
nntp	119	tcp	Network News Transfer Protocol
nntp	119	udp	Network News Transfer Protocol
cfdpkt	120	tcp	CFDPTKT
cfdpkt	120	udp	CFDPTKT
erpc	121	tcp	Encore Expedited Remote Pro.Call
erpc	121	udp	Encore Expedited Remote Pro.Call
smakynet	122	tcp	SMAKYNET
smakynet	122	udp	SMAKYNET
ntp	123	tcp	Network Time Protocol
ntp	123	udp	Network Time Protocol

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
ansatrader	124	tcp	ANSA REX Trader
ansatrader	124	udp	ANSA REX Trader
locus-map	125	tcp	Locus PC-Interface Net. Map Ser
locus-map	125	udp	Locus PC-Interface Net. Map Ser
nxedit	126	tcp	NXEdit
nxedit	126	udp	NXEdit
locus-con	127	tcp	Locus PC-Interface Conn. Server
locus-con	127	udp	Locus PC-Interface Conn. Server
gss-xlicen	128	tcp	GSS X License Verification
gss-xlicen	128	udp	GSS X License Verification
pwdgen	129	tcp	Password Generator Protocol
pwdgen	129	udp	Password Generator Protocol
cisco-fna	130	tcp	Cisco FNATIVE
cisco-fna	130	udp	Cisco FNATIVE
cisco-tna	131	tcp	Cisco TNATIVE
cisco-tna	131	udp	Cisco TNATIVE
cisco-sys	132	tcp	Cisco SYSMANT
cisco-sys	132	udp	Cisco SYSMANT
statsrv	133	tcp	Statistics Service
statsrv	133	udp	Statistics Service
ingres-net	134	tcp	INGRES-NET Service
ingres-net	134	udp	INGRES-NET Service
epmap	135	tcp	DCE Endpoint Resolution
epmap	135	udp	DCE Endpoint Resolution
profile	136	tcp	PROFILE Naming System
profile	136	udp	PROFILE Naming System
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service

Serviciu	Număr de port	Protocol	Descriere
netbios-dgm	138	tcp	NETBIOS Datagram Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
netbios-ssn	139	udp	NETBIOS Session Service
emfis-data	140	tcp	EMFIS Data Service
emfis-data	140	udp	EMFIS Data Service
emfis-cntl	141	tcp	EMFIS Control Service
emfis-cntl	141	udp	EMFIS Control Service
bl-idm	142	tcp	Britton-Lee IDM
bl-idm	142	udp	Britton-Lee IDM
imap	143	tcp	Internet Message Access Protocol
imap	143	udp	Internet Message Access Protocol
uma	144	tcp	Universal Management Architecture
uma	144	udp	Universal Management Architecture
uaac	145	tcp	UAAC Protocol
uaac	145	udp	UAAC Protocol
iso-tp0	146	tcp	ISO-IP0
iso-tp0	146	udp	ISO-IP0
iso-ip	147	tcp	ISO-IP
iso-ip	147	udp	ISO-IP
jargon	148	tcp	Jargon
jargon	148	udp	Jargon
aed-512	149	tcp	AED 512 Emulation Service
aed-512	149	udp	AED 512 Emulation Service
sql-net	150	tcp	SQL-NET
sql-net	150	udp	SQL-NET
hems	151	tcp	HEMS
hems	151	udp	FiEMS
bftp	152	tcp	Background File Transfer Program

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
bftp	152	udp	Background File Transfer Program
sgmp	153	tcp	SGMP
sgmp	153	udp	SGMP
netsc-prod	154	tcp	NETSC
netsc-prod	154	udp	NETSC
netsc-dev	155	tcp	NETSC
netsc-dev	155	udp	NETSC
sqlsrv	156	tcp	SQL Service
sqlsrv	156	udp	SQL Service
knet-cmp	157	tcp	KNET VM Command Message Protocol
knet-cmp	157	udp	KNET VM Command Message Protocol
pcmail-srv	158	tcp	PCMail Server
pcmail-srv	158	udp	PCMail Server
nss-routing	159	tcp	NSS-Routing
nss-routing	159	udp	NSS-Routing
sgmp-traps	160	tcp	SGMP-TRAPS
sgmp-traps	160	udp	SGMP-TRAPS
snmp	161	tcp	SNMP
snmp	161	udp	SNMP
snmptrap	162	tcp	SNMPTRAP
snmptrap	162	udp	SNMPTRAP
cmip-man	163	tcp	CMIP TCP Manager
cmip-man	163	udp	CMIP TCP Manager
cmip-agent	164	tcp	CMIP TCP Agent
cmip-agent	164	udp	CMIP TCP Agent
xns-courier	165	tcp	Xerox
xns-courier	165	udp	Xerox
s-net	166	tcp	Sirius Systems

Serviciu	Număr de port	Protocol	Descriere
s-net	166	udp	Sirius Systems
namp	167	tcp	NAMP
namp	167	udp	NAMP
rsvd	168	tcp	RSVD
rsvd	168	udp	RSVD
send	169	tcp	SEND
send	169	udp	SEND
print-srv	170	tcp	Network PostScript
print-srv	170	udp	Network PostScript
multiplex	171	tcp	Network Innovations Multiplex
multiplex	171	udp	Network Innovations Multiplex
cl/1	172	tcp	Network Innovations CL/1
cl/1	172	udp	Network Innovations CL/1
xyplex-mux	173	tcp	Xyplex
xyplex-mux	173	udp	Xyplex
mailq	174	tcp	MAILQ
mailq	174	udp	MAILQ
vmnet	175	tcp	VMNET
vmnet	175	udp	VMNET
genrad-mux	176	tcp	GENRAD-MUX
genrad-mux	176	udp	GENRAD-MUX
xdmcp	177	tcp	X Display Manager Control Protocol
xdmcp	177	udp	X Display Manager Control Protocol
nextstep	178	tcp	NextStep Window Server
nextstep	178	udp	NextStep Window Server
bgp	179	tcp	Border Gateway Protocol
bgp	179	udp	Border Gateway Protocol
ris	180	tcp	Intergraph
ris	180	udp	Intergraph

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
unify	181	tcp	Unify
unify	181	udp	Unify
audit	182	tcp	Unisys Audit SITP
audit	182	udp	Unisys Audit SITP
ocbinder	183	tcp	OCBinder
ocbinder	183	udp	OCBinder
ocserver	184	tcp	OCServer
ocserver	184	udp	OCServer
remote-kis	185	tcp	Remote-KIS
remote-kis	185	udp	Remote-KIS
kis	186	tcp	KIS Protocol
kis	186	udp	KIS Protocol
aci	187	tcp	Application Communication Interface
aci	187	udp	Application Communication Interface
mumps	188	tcp	Plus Five's MUMPS
mumps	188	udp	Plus Five's MUMPS
qft	189	tcp	Queued File Transport
qft	189	udp	Queued File Transport
gacp	190	tcp	Gateway Access Control Protocol
gacp	190	udp	Gateway Access Control Protocol
prospero	191	tcp	Prospero Directory Service
prospero	191	udp	Prospero Directory Service
osu-nms	192	tcp	OSU Network Monitoring System
osu-nms	192	udp	OSU Network Monitoring System
srmp	193	tcp	Spider Remote Monitoring Protocol
srmp	193	udp	Spider Remote Monitoring Protocol
irc	194	tcp	Internet Relay Chat Protocol
irc	194	udp	Internet Relay Chat Protocol

Serviciu	Număr de port	Protocol	Descriere
dn6-nlm-aud	195	tcp	DNSIX Network Level Module Audit
dnb-nlm-aud	195	udp	DNSIX Network Level Module Audit
dn6-smm-red	196	tcp	DNSIX Session Mgt. Module Audit Redir
dn6-smm-red	196	udp	DNSIX Session Mgt. Module Audit Redir
dls	197	tcp	Directory Location Service
dls	197	udp	Directory Location Service
dls-mon	198	tcp	Directory Location Service Monitor
dls-mon	198	udp	Directory Location Service Monitor
smux	199	tcp	SMUX
smux	199	udp	SMUX
src	200	tcp	IBM System Resource Controller
src	200	udp	IBM System Resource Controller
at-rtmp	201	tcp	AppleTalk Routing Maintenance
at-rtmp	201	udp	AppleTalk Routing Maintenance
at-nbp	202	tcp	AppleTalk Name Binding
at-nbp	202	udp	AppleTalk Name Binding
at-3	203	tcp	AppleTalk Unused
at-3	203	udp	AppleTalk Unused
at-echo	204	tcp	AppleTalk Echo
at-echo	204	udp	AppleTalk Echo
at-5	205	tcp	AppleTalk Unused
at-5	205	udp	AppleTalk Unused
at-zis	206	tcp	AppleTalk Zone Information
at-zis	206	udp	AppleTalk Zone Information
at-7	207	tcp	AppleTalk Unused
at-7	207	udp	AppleTalk Unused
at-8	208	tcp	AppleTalk Unused
at-8	208	udp	AppleTalk Unused

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
qmtpt	209	tcp	The Quick Mail Transfer Protocol
qmtpt	209	udp	The Quick Mail Transfer Protocol
z39.50	210	tcp	ANSI Z39.50
z39.50	210	udp	ANSI Z39.50
914c/g	211	tcp	Texas Instruments 914C/G Terminal
914c/g	211	udp	Texas Instruments 914C/G Terminal
anet	212	tcp	ATEXSSTR
anet	212	udp	ATEXSSTR
ipx	213	tcp	IPX
ipx	213	udp	IPX
vmpwscs	214	tcp	VM PWSCS
vmpwscs	214	udp	VM PWSCS
softpc	215	tcp	Insignia Solutions
softpc	215	udp	Insignia Solutions
CAIlic	216	tcp	Computer Associates Int'l. License Server
CAIlic	216	udp	Computer Associates Int'l License Server
dbase	217	tcp	dBASE UNIX
dbase	217	udp	dBASE UNIX
mpp	218	tcp	Netix Message Posting Protocol
mpp	218	udp	Netix Message Posting Protocol
uarps	219	tcp	Unisys ARPs
uarps	219	udp	Unisys ARPs
imap3	220	tcp	Interactive Mail Access Protocol v3
imap3	220	udp	Interactive Mail Access Protocol v3
fln-spx	221	tcp	Berkeley rlogind with SPX
authfln-spx	221	udp	Berkeley rlogind with SPX
authrsh-spx	222	tcp	Berkeley rshd with SPX auth.
rsh-spx	222	udp	Berkeley rshd with SPX auth.

Serviciu	Număr de port	Protocol	Descriere
cde	223	tcp	Certificate Distribution Center
cde	223	udp	Certificate Distribution Center
masqdiater	224	tcp	masqdiater
masqdiater	224	udp	masqdiater
direct	242	tcp	Direct
direct	242	udp	Direct
sur-meas	243	tcp	Survey Measurement
sur-meas	243	udp	Survey Measurement
dayna	244	tcp	Dayna
dayna	244	udp	Dayna
link	245	tcp	LINK
link	245	udp	LINK
dsp3270	246	tcp	Display Systems Protocol
dsp3270	246	udp	Display Systems Protocol
subntbcst_tftp	247	tcp	SUBNTBCST_TFTP
subntbcst_tftp	247	udp	SUBNTBCST_TFTP
bhfhs	248	tcp	bhfhs
bhfhs	248	udp	bhfhs
rap	256	tcp	RAP
rap	256	udp	RAP
set	257	tcp	Secure Electronic Transaction
set	257	udp	Secure Electronic Transaction
yak-chat	258	tcp	Yak Winsock Personal Chat
yak-chat	258	udp	Yak Winsock Personal Chat
esro-gen	259	tcp	Efficient Short Remote Operations
esro-gen	259	udp	Efficient Short Remote Operations
openport	260	tcp	Openport
openport	260	udp	Openport
nsiiops	261	tcp	IIOP Name Service over TLS/SSL

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
nsiops	261	udp	IIOF Name Service over TLS/SSL
arcisdms	262	tcp	Arcisdms
arcisdms	262	udp	Arcisdms
hdap	263	tcp	HDAP
hdap	263	udp	HDAP
bgmp	264	tcp	BGMP
bgmp	264	udp	BGMP
http-mgmt	280	tcp	http-mgmt
http-mgmt	280	udp	http-mgmt
personal-link	281	tcp	Personal Link
personal-link	281	udp	Personal Link
cableport-ax	282	tcp	Cable Port AX
cableport-ax	282	udp	Cable Port AX
rescap	283	tcp	Rescap
rescap	283	udp	Rescap
novastorbakup	308	tcp	Novastor Backup
novastorbakup	308	udp	Novastor Backup
entrusttime	309	tcp	EntrustTime
entrusttime	309	udp	EntrustTime
bhmds	310	tcp	bhmds
bhmds	310	udp	bhmds
asip-webadmin	311	tcp	AppleShare IP WebAdmin
asip-webadmin	311	udp	AppleShare IP WebAdmin
vslmp	312	tcp	VSLMP
vslmp	312	udp	VSLMP
magenta-logic	313	tcp	Magenta Logic
magenta-logic	313	udp	Magenta Logic
opalis-robot	314	tcp	Opalis Robot

Serviciu	Număr de port	Protocol	Descriere
opalis-robot	314	udp	Opalis Robot
dpsi	315	tcp	DPSI
dpsi	315	udp	DPSI
decauth	316	tcp	decAuth
decauth	316	udp	decAuth
zannet	317	tcp	Zannet
zannet	317	udp	Zannet
pkix-timestamp	318	tcp	PKIX TimeStamp
pkix-timestamp	318	udp	PKIX TimeStamp
ptp-event	319	tcp	PTP Event
ptp-event	319	udp	PTP Event
ptp-general	320	tcp	PTP General
ptp-general	320	udp	PTP General
pip	321	tcp	PIP
pip	321	udp	PIP
rtsp	322	tcp	RTSPS
rtsp	322	udp	RTSPS
pdap	344	tcp	Prospero Data Access Protocol
pdap	344	udp	Prospero Data Access Protocol
pawserv	345	tcp	Perf Analysis Workbench
pawserv	345	udp	Perf Analysis Workbench
zserv	346	tcp	Zebra Server
zserv	346	udp	Zebra Server
faterv	347	tcp	Fatmen Server
faterv	347	udp	Fatmen Server
csi-sgwp	348	tcp	Cabletron Management Protocol
csi-sgwp	348	udp	Cabletron Management Protocol
mftp	349	tcp	mftp
mftp	349	udp	mftp

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
matip-type-a	350	tcp	MATIP Type A
matip-type-a	350	udp	MATIP Type A
matip-type-b	351	tcp	MATIP Type B
matip-type-b	351	udp	MATIP Type B
bhoetty	351	tcp	bhoetty
bhoetty	351	udp	bhoetty
dtag-ste-sb	352	tcp	DTAG
dtag-ste-sb	352	udp	DTAG
bhoedap4	352	tcp	bhoedap4
bhoedap4	352	udp	bhoedap4
ndsauth	353	tcp	NDSAUTH
ndsauth	353	udp	NDSAUTH
bh611	354	tcp	bh611
bh611	354	udp	bh611
datex-asn	355	tcp	DATEX-ASN
datex-asn	355	udp	DATEX-ASN
cloanto-net-1	356	tcp	Cloanto Net 1
cloanto-net-1	356	udp	Cloanto Net 1
bhevent	357	tcp	bhevent
bhevent	357	udp	bhevent
shrinkwrap	358	tcp	Shrinkwrap
shrinkwrap	358	udp	Shrinkwrap
tenebris_nts	359	tcp	Tenebris Network Trace Service
tenebris_nts	359	udp	Tenebris Network Trace Service
scoi2odialog	360	tcp	scoi2odialog
scoi2odialog	360	udp	scoi2odialog
semantix	361	tcp	Semantix
semantix	361	udp	Semantix

Serviciu	Număr de port	Protocol	Descriere
srssend	362	tcp	SRS Send
srssend	362	udp	SRS Send
rsvp_tunnel	363	tcp	RSVP Tunnel
rsvp_tunnel	363	udp	RSVP Tunnel
aurora-cmgr	364	tcp	Aurora CMGR
aurora-cmgr	364	udp	Aurora CMGR
dtk	365	tcp	DTK
dtk	365	udp	DTK
odmr	366	tcp	ODMR
odmr	366	udp	ODMR
mortgageware	367	tcp	MortgageWare
mortgageware	367	udp	MortgageWare
qbikgdp	368	tcp	QbikGDP
qbikgdp	368	udp	QbikGDP
rpc2portmap	369	tcp	rpc2portmap
rpc2portmap	369	udp	rpc2portmap
codaaauth2	370	tcp	codaaauth2
codaaauth2	370	udp	codaaauth2
clearcase	371	tcp	Clearcase
clearcase	371	udp	Clearcase
ulistproc	372	tcp	ListProcessor
ulistproc	372	udp	ListProcessor
legent-1	373	tcp	Legent Corporation
legent-1	373	udp	Legent Corporation
legent-2	374	tcp	Legent Corporation
legent-2	374	udp	Legent Corporation
hassle	375	tcp	Hassle
hassle	375	udp	Hassle
nip	376	tcp	Amiga Envoy Network Inquiry Proto

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
nip	376	udp	Amiga Envoy Network Inquiry Proto
tnETOS	377	tcp	NEC Corporation
tnETOS	377	udp	NEC Corporation
dsETOS	378	tcp	NEC Corporation
dsETOS	378	udp	NEC Corporation
is99c	379	tcp	TIA/EIA/IS-99 Modem Client
is99c	379	udp	TIA/EIA/IS-99 Modem Client
is99s	380	tcp	TIA/EIA/IS-99 Modem Server
is99s	380	udp	TIA/EIA/IS-99 Modem Server
hp-collector	381	tcp	hp Performance Data Collector
hp-collector	381	udp	hp Performance Data Collector
hp-managed-node	382	tcp	hp Performance Data Managed Node
hp-managed-node	382	udp	hp Performance Data Managed Node
hp-alarm-mgr	383	tcp	hp Performance Data Alarm Manager
hp-alarm-mgr	383	udp	hp Performance Data Alarm Manager
arns	384	tcp	A Remote Network Server System
arns	384	udp	A Remote Network Server System
ibm-app	385	tcp	IBM Application
ibm-app	385	udp	IBM Application
asa	386	tcp	ASA Message Router Object Def.
asa	386	udp	ASA Message Router Object Def.
aurp	387	tcp	Appletalk Update-Based Routing Pro.
aurp	387	udp	Appletalk Update-Based Routing Pro.
unidata-ldm	388	tcp	Unidata LDM Version 4
unidata-ldm	388	udp	Unidata LDM Version 4
ldap	389	tcp	Lightweight Directory Access Protocol
ldap	389	udp	Lightweight Directory Access Protocol

Serviciu	Număr de port	Protocol	Descriere
uis	390	tcp	UIS
uis	390	udp	UIS
synotics-relay	391	tcp	SynOptics SNMP Relay Port
synotics-relay	391	udp	SynOptics SNMP Relay Port
synotics-broker	392	tcp	SynOptics Port Broker Port
synotics-broker	392	udp	SynOptics Port Broker Port
dis	393	tcp	Data Interpretation System
dis	393	udp	Data Interpretation System
embl-ndt	394	tcp	EMBL Nucleic Data Transfer
embl-ndt	394	udp	EMBL Nucleic Data Transfer
netcp	395	tcp	NETscout Control Protocol
netcp	395	udp	NETscout Control Protocol
netware-ip	396	tcp	Novell Netware over IP
netware-ip	396	udp	Novell Netware over IP
mptn	397	tcp	Multi Protocol Trans. Net.
mptn	397	udp	Multi Protocol Trans. Net.
kryptolan	398	tcp	Kryptolan
kryptolan	398	udp	Kryptolan
iso-tsap-c2	399	tcp	ISO Transport Class 2 Non-Control over TCP
iso-tsap-c2	399	udp	ISO Transport Class 2 Non-Control over TCP
work-sol	400	tcp	Workstation Solutions
work-sol	400	udp	Workstation Solutions
ups	401	tcp	Uninterruptible Power Supply
ups	401	udp	Uninterruptible Power Supply
genie	402	tcp	Genie Protocol
genie	402	udp	Genie Protocol
decap	403	tcp	decap
decap	403	udp	decap
nced	404	tcp	nced

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
nced	404	udp	nced
ncld	405	tcp	ncld
ncld	405	udp	ncld
imsp	406	tcp	Interactive Mail Support Protocol
imsp	406	udp	Interactive Mail Support Protocol
timbuktu	407	tcp	Timbuktu
timbuktu	407	udp	Timbuktu
prm-sm	408	tcp	Prospero Resource Manager Sys. Man.
prm-sm	408	udp	Prospero Resource Manager Sys. Man.
prm-nm	409	tcp	Prospero Resource Manager Node Man.
prm-nm	409	udp	Prospero Resource Manager Node Man.
decladebug	410	tcp	DECLadebug Remote Debug Protocol
decladebug	410	udp	DECLadebug Remote Debug Protocol
rmt	411	tcp	Remote MT Protocol
rmt	411	udp	Remote MT Protocol
synoptics-trap	412	tcp	Trap Convention Port
synoptics-trap	412	udp	Trap Convention Port
smssp	413	tcp	SMSP
smssp	413	udp	SMSP
infoseek	414	tcp	InfoSeek
infoseek	414	udp	InfoSeek
bnet	415	tcp	BNet
bnet	415	udp	BNet
silverplatter	416	tcp	Silverplatter
silverplatter	416	udp	Silverplatter
onmux	417	tcp	Onmux
onmux	417	udp	Onmux
hyper-g	418	tcp	Hyper-G

Serviciu	Număr de port	Protocol	Descriere
hyper-g	418	udp	Hyper-G
ariel1	419	tcp	Ariel
ariel1	419	udp	Ariel
smpte	420	tcp	SMPTE
smpte	420	udp	SMPTE
ariel2	421	tcp	Ariel
ariel2	421	udp	Ariel
ariel3	422	tcp	Ariel
ariel3	422	udp	Ariel
opc-job-start	423	tcp	IBM Operations Planning and Control Start
opc-job-start	423	udp	IBM Operations Planning and Control Start
opc-job-track	424	tcp	IBM Operations Planning and Control Track
opc-job-track	424	udp	IBM Operations Planning and Control Track
icad-el	425	tcp	ICAD
icad-el	425	udp	ICAD
smartsdp	426	tcp	smartsdp
smartsdp	426	udp	smartsdp
svrloc	427	tcp	Server Location
svrloc	427	udp	Server Location
ocs_cmu	428	tcp	OCS_CMU
ocs_cmu	428	udp	OCS_CMU
ocs_amu	429	tcp	OCS_AMU
ocs_amu	429	udp	OCS_AMU
utmpsd	430	tcp	UTMPD
utmpsd	430	udp	UTMPD
utmpcd	431	tcp	UTMPCD
utmpcd	431	udp	UTMPCD
iasd	432	tcp	IASD
iasd	432	udp	IASD

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
nnsdp	433	tcp	NNSP
nnsdp	433	udp	NNSP
mobileip-agent	434	tcp	MobileIP-Agent
mobileip-agent	434	udp	MobileIP-Agent
mobilip-mn	435	tcp	MobilIP-MN
mobilip-mn	435	udp	MobilIP-MN
dna-cml	436	tcp	DNA-CML
dna-cml	436	udp	DNA-CML
comscm	437	tcp	comscm
comscm	437	udp	comscm
dsfgw	438	tcp	dsfgw
dsfgw	438	udp	dsfgw
dasp	439	tcp	dasp
dasp	439	udp	dasp
sgcp	440	tcp	sgcp
sgcp	440	udp	sgcp
decvms-sysmgt	441	tcp	decvms-sysmgt
decvms-sysmgt	441	udp	decvms-sysmgt
cvc_hostd	442	tcp	cvc_hostd
cvc_hostd	442	udp	cvc_hostd
https	443	tcp	http protocol over TLS/SSL
https	443	udp	http protocol over TLS/SSL
snpp	444	tcp	Simple Network Paging Protocol
snpp	444	udp	Simple Network Paging Protocol
microsoft-ds	445	tcp	Microsoft-DS
microsoft-ds	445	udp	Microsoft-DS
ddm-rdb	446	tcp	DDM-RDB
ddm-rdb	446	udp	DDM-RDB

Serviciu	Număr de port	Protocol	Descriere
ddm-dfm	447	tcp	DDM-RFM
ddm-dfm	447	udp	DDM-RFM
ddm-ssl	448	tcp	DDM-SSL
ddm-ssl	448	udp	DDM-SSL
as-servermap	449	tcp	AS Server Mapper
as-servermap	449	udp	AS Server Mapper
tserver	450	tcp	TServer
tserver	450	udp	TServer
sfs-smp-net	451	tcp	Cray Network Semaphore Server
sfs-smp-net	451	udp	Cray Network Semaphore Server
sfs-config	452	tcp	Cray SFS Config Server
sfs-config	452	udp	Cray SFS Config Server
creativeserver	453	tcp	CreativeServer
creativeserver	453	udp	CreativeServer
contentserver	454	tcp	ContentServer
contentserver	454	udp	ContentServer
creativepartnr	455	tcp	CreativePartnr
creativepartnr	455	udp	CreativePartnr
macon-tcp	456	tcp	macon-tcp
macon-udp	456	udp	macon-udp
scohelp	457	tcp	scohelp
scohelp	457	udp	scohelp
appleqt	458	tcp	Apple Quick Time
appleqt	458	udp	Apple Quick Time
ampr-rcmd	459	tcp	ampr-rcmd
ampr-rcmd	459	udp	ampr-rcmd
skronk	460	tcp	skronk
skronk	460	udp	skronk
datasurfsrv	461	tcp	DataRampSrv

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
datasurfsrv	461	udp	DataRampSrv
datasurfsrvsec	462	tcp	DataRampSrvSec
datasurfsrvsec	462	udp	DataRampSrvSec
alpes	463	tcp	alpes
alpes	463	udp	alpes
kpasswd	464	tcp	kpasswd
kpasswd	464	udp	kpasswd
digital-vrc	466	tcp	digital-vrc
digital-vrc	466	udp	digital-vrc
mylex-mapd	467	tcp	mylex-mapd
mylex-mapd	467	udp	mylex-mapd
photuris	468	tcp	proturis
photuris	468	udp	proturis
rcp	469	tcp	Radio Control Protocol
rcp	469	udp	Radio Control Protocol
scx-proxy	470	tcp	scx-proxy
scx-proxy	470	udp	scx-proxy
mondex	471	tcp	Mondex
mondex	471	udp	Mondex
ljk-login	472	tcp	ljk-login
ljk-login	472	udp	ljk-login
hybrid-pop	473	tcp	hybrid-pop
hybrid-pop	473	udp	hybrid-pop
tn-tl-w1	474	tcp	tn-tl-w1
tn-tl-w2	474	udp	tn-tl-w2
tcpnethaspsrv	475	tcp	tcpnethaspsrv
tcpnethaspsrv	475	udp	tcpnethaspsrv
tn-tl-fd1	476	tcp	tn-tl-fd1

Serviciu	Număr de port	Protocol	Descriere
tn-tl-fd1	476	udp	tn-tl-fd1
ss7ns	477	tcp	ss7ns
ss7ns	477	udp	ss7ns
spsc	478	tcp	spsc
spsc	478	udp	spsc
iafserver	479	tcp	iafserver
iafserver	479	udp	iafserver
iafdbase	480	tcp	iafdbase
iafdbase	480	udp	iafdbase
ph	481	tcp	Ph service
ph	481	udp	Ph service
bgs-nsi	482	tcp	bgs-nsi
bgs-nsi	482	udp	bgs-nsi
ulpnet	483	tcp	ulpnet
ulpnet	483	udp	ulpnet
integra-sme	484	tcp	Integra Software Management Environment
integra-sme	484	udp	Integra Software Management Environment
powerburst	485	tcp	Air Soft Power Burst
powerburst	485	udp	Air Soft Power Burst
avian	486	tcp	avian
avian	486	udp	avian
saft	487	tcp	saft Simple Asynchronous File Transfer
saft	487	udp	saft Simple Asynchronous File Transfer
gss-http	488	tcp	gss-http
gss-http	488	udp	gss-http
nest-protocol	489	tcp	nest-protocol
nest-protocol	489	udp	nest-protocol
micom-pfs	490	tcp	micom-pfs
micom-pfs	490	udp	micom-pfs

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
go-login	491	tcp	go-login
go-login	491	udp	go-login
ticf-1	492	tcp	Transport Independent Convergence for FNA
ticf-1	492	udp	Transport Independent Convergence for FNA
ticf-2	493	tcp	Transport Independent Convergence for FNA
ticf-2	493	udp	Transport Independent Convergence for FNA
pov-ray	494	tcp	POV-Ray
pov-ray	494	udp	POV-Ray
intecourier	495	tcp	intecourier
intecourier	495	udp	intecourier
pim-rp-disc	496	tcp	PIM-RP-DISC
pim-rp-disc	496	udp	PIM-RP-DISC
dantz	497	tcp	dantz
dantz	497	udp	dantz
siam	498	tcp	siam
siam	498	udp	siam
iso-ill	499	tcp	ISO ILL Protocol
iso-ill	499	udp	ISO ILL Protocol
isakmp	500	tcp	isakmp
isakmp	500	udp	isakmp
stmf	501	tcp	STMF
stmf	501	udp	STMF
asa-appl-proto	502	tcp	asa-appl-proto
asa-appl-proto	502	udp	asa-appl-proto
intrinsa	503	tcp	Intrinsa
intrinsa	503	udp	Intrinsa
citadel	504	tcp	citadel
citadel	504	udp	citadel

Serviciu	Număr de port	Protocol	Descriere
mailbox-lm	505	tcp	mailbox-lm
mailbox-lm	505	udp	mailbox-lm
ohimsrv	506	tcp	ohimsrv
ohimsrv	506	udp	ohimsrv
crs	507	tcp	crs
crs	507	udp	crs
xvttp	508	tcp	xvttp
xvttp	508	udp	xvttp
snare	509	tcp	snare
snare	509	udp	snare
fcp	510	tcp	FirstClass Protocol
fcp	510	udp	FirstClass Protocol
passgo	511	tcp	PassGo
passgo	511	udp	PassGo
exec	512	tcp	execuție de procese de la distanță
comsat	512	udp	
biff	512	udp	Folosit de sistemul de poștă pentru informarea utilizatorilor
login	513	tcp	Conectare de la distanță la Telnet
who	513	udp	Întreține bazele de date who is
shell	514	tcp	cmd
syslog	514	udp	
printer	515	tcp	spooler
printer	515	udp	spooler
videotex	516	tcp	videotex
videotex	516	udp	videotex
talk	517	tcp	La fel ca legătura tenex, dar încrucișat
talk	517	udp	La fel ca legătura tenex, dar încrucișat
ntalk	518	tcp	

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
ntalk	518	udp	
utime	519	tcp	unixtime
utime	519	udp	unixtime
efs	520	tcp	Extended File Name Server
router	520	udp	Local Routing Process (on site)
ripng	521	tcp	ripng
ripng	521	udp	ripng
ulp	522	tcp	ULP
ulp	522	udp	ULP
ibm-db2	523	tcp	IBM-DB2
ibm-db2	523	udp	IBM-DB2
ncp	524	tcp	NCP
ncp	524	udp	NCP
timed	525	tcp	timeserver
timed	525	udp	timeserver
tempo	526	tcp	newdate
tempo	526	udp	newdate
stx	527	tcp	Stock IXChange
stx	527	udp	Stock IXChange
custix	528	tcp	Customer IXChange
custix	528	udp	Customer IXChange
irc-serv	529	tcp	IRC-SERV
irc-serv	529	udp	IRC-SERV
courier	530	tcp	rpc
courier	530	udp	rpc
conference	531	tcp	chat
conference	531	udp	chat
netnews	532	tcp	readnews

Serviciu	Număr de port	Protocol	Descriere
netnews	532	udp	readnews
netwall	533	tcp	Pentru difuzări de urgență
netwall	533	udp	Pentru difuzări de urgență
mm-admin	534	tcp	MegaMedia Admin
mm-admin	534	udp	MegaMedia Admin
iiop	535	tcp	iiop
iiop	535	udp	iiop
opalis-rdv	536	tcp	opalis-rdv
opalis-rdv	536	udp	opalis-rdv
nmosp	537	tcp	Networked Media Streaming Protocol
nmosp	537	udp	Networked Media Streaming Protocol
gdomap	538	tcp	gdomap
gdomap	538	udp	gdomap
apertus-ldp	539	tcp	Apertus Technologies Load Determination
apertus-ldp	539	udp	Apertus Technologies Load Determination
uucp	540	tcp	uucpd
uucp	540	udp	uucpd
uucp-rlogin	541	tcp	uucp-rlogin
uucp-rlogin	541	udp	uucp-rlogin
commerce	542	tcp	commerce
commerce	542	udp	commerce
klogin	543	tcp	
klogin	543	udp	
kshell	544	tcp	krcmd
kshell	544	udp	krcmd
appleqtcsrvr	545	tcp	appleqtcsrvr
appleqtcsrvr	545	udp	appleqtcsrvr
dhcpv6-client	546	tcp	DHCPv6 Client
dhcpv6-client	54b	udp	DHCPv6 Client

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
dhcpv6-server	547	tcp	DHCPv6 Server
dhcpv6-server	547	udp	DHCPv6 Server
afpovertcp	548	tcp	AFP over TCP
afpovertcp	548	udp	AFP over TCP
idfp	549	tcp	IDFP
idfp	549	udp	IDFP
new-rwho	550	tcp	new-who
new-rwho	550	udp	new-who
cybercash	551	tcp	cybercash
cybercash	551	udp	cybercash
deviceshare	552	tcp	deviceshare
deviceshare	552	udp	deviceshare
pirp	553	tcp	pirp
pirp	553	udp	pirp
rtsp	554	tcp	Real Time Stream Control Protocol
rtsp	554	udp	Real Time Stream Control Protocol
dsf	555	tcp	
dsf	555	udp	
remotefs	556	tcp	rfs server
remotefs	556	udp	rfs server
openvms-sysipc	557	tcp	openvms-sysipc
openvms-sysipc	557	udp	openvms-sysipc
sdnskmp	558	tcp	SDNSKMP
sdnskmp	558	udp	SDNSKMP
teedtap	559	tcp	TEEDTAP
teedtap	559	udp	TEEDTAP
rmonitor	560	tcp	rmonitord
rmonitor	560	udp	rmonitord

Serviciu	Număr de port	Protocol	Descriere
monitor	561	tcp	
monitor	561	udp	
chshell	562	tcp	chcmd
chshell	562	udp	chcmd
nntps	563	tcp	protocolul nntp peste TLS/SSL (fost snntp)
nntps	563	udp	protocolul nntp peste TLS/SSL (fost snntp)
9pfs	564	tcp	Plan 9 File Service
9pfs	564	udp	Plan 9 File Service
whoami	565	tcp	whoami
whoami	565	udp	whoami
streettalk	566	tcp	streettalk
streettalk	566	udp	streettalk
banyan-rpc	567	tcp	banyan-rpc
banyan-rpc	567	udp	banyan-rpc
ms-shuttle	568	tcp	microsoft shuttle
ms-shuttle	568	udp	microsoft shuttle
ms-rome	569	tcp	microsoft rome
ms-rome	569	udp	microsoft rome
meter	570	tcp	demon
meter	570	udp	demon
meter	571	tcp	udemon
meter	571	udp	udemon
sonar	572	tcp	sonar
sonar	572	udp	sonar
banyan-vip	573	tcp	banyan-vip
banyan-vip	573	udp	banyan-vip
ftp-agent	574	tcp	FTP Software Agent System
ftp-agent	574	udp	FTP SofMare Agent System
vemmi	575	tcp	VEMMI

Universitatea Tehnică Iași
BIBLIOTECA

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
vemmi	575	udp	VEMMI
ipcd	576	tcp	ipcd
ipcd	576	udp	ipcd
vnas	577	tcp	vnas
vnas	577	udp	vnas
ipdd	578	tcp	ipdd
ipdd	578	udp	ipdd
decbsrv	579	tcp	decbsrv
decbsrv	579	udp	decbsrv
sntp-heartbeat	580	tcp	SNTP HEARTBEAT
sntp-heartbeat	580	udp	SNTP HEARTBEAT
bdp	581	tcp	Bundle Discovery Protocol
bdp	581	udp	Bundle Discovery Protocol
scc-security	582	tcp	SCC Security
scc-security	582	udp	SCC Security
philips-vc	583	tcp	Philips Video-Conferencing
philips-vc	583	udp	Philips Video-Conferencing
keyserver	584	tcp	Key Server
keyserver	584	udp	Key Server
imap4-ssl	585	tcp	IMAP4+SSL (folosește 993)
imap4-ssl	585	udp	IMAP4+SSL (folosește 993)
password-chg	586	tcp	Password Change
password-chg	586	udp	Password Change
submission	587	tcp	Submission
submission	587	udp	Submission
cal	588	tcp	CAL
cal	588	udp	CAL
eyelink	589	tcp	EyeLink

Serviciu	Număr de port	Protocol	Descriere
eyelink	589	udp	EyeLink
tns-cml	590	tcp	TNS CML
tns-cml	590	udp	TNS CML
http-alt	591	tcp	FileMaker, Inc. – HTTP Alternate (vezi Port 80)
http-alt	591	udp	FileMaker, Inc. – HTTP Alternate (vezi Port 80)
eudora-set	592	tcp	Eudora Set
eudora-set	592	udp	Eudora Set
http-rpc-epmap	593	tcp	HTTP RPC Ep Map
http-rpc-epmap	593	udp	HTTP RPC Ep Map
tpip	594	tcp	TPIP
tpip	594	udp	TPIP
cab-protocol	595	tcp	CAB Protocol
cab-protocol	595	udp	CAB Protocol
smsd	596	tcp	SMSD
smsd	596	udp	SMSD
ptcnameservice	597	tcp	PTC Name Service
ptcnameservice	597	udp	PTC Name Service
sco-websrvrmg3	598	tcp	SCO Web Server Manager 3
sco-websrvrmg3	598	udp	SCO Web Server Manager 3
acp	599	tcp	Aeolon Core Protocol
acp	599	udp	Aeolon Core Protocol
ipcserver	600	tcp	Sun IPC server
ipcserver	600	udp	Sun IPC server
urm	606	tcp	Cray Unified Resource Manager
urm	606	udp	Cray Unified Resource Manager
nqs	607	tcp	nqs
nqs	607	udp	nqs
sift-uft	608	tcp	Sender-Initiated/Unsolicited File Transfer
sift-uft	608	udp	Sender-Initiated/Unsolicited File Transfer

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
npmp-trap	609	tcp	npmp-trap
npmp-trap	609	udp	npmp-trap
npmp-local	610	tcp	npmp-local
npmp-local	610	udp	npmp-local
npmp-gui	611	tcp	npmp-gui
npmp-gui	611	udp	npmp-gui
hmmp-ind	612	tcp	HMMP Indication
hmmp-ind	612	udp	HMMP Indication
hmmp-op	613	tcp	HMMP Operation
hmmp-op	613	udp	HMMP Operation
sshell	614	tcp	SSLshell
sshell	614	udp	SSLshell
sco-inetmgr	615	tcp	Internet Configuration Manager
sco-inetmgr	615	udp	Internet Configuration Manager
sco-sysmgr	616	tcp	SCO System Administration Server
sco-sysmgr	616	udp	SCO System Administration Server
sco-dtmgr	617	tcp	SCO Desktop Administration Server
sco-dtmgr	617	udp	SCO Desktop Administration Server
dei-icda	618	tcp	DEI-ICDA
dei-icda	618	udp	DEI-ICDA
digital-evm	619	tcp	Digital EVM
digital-evm	619	udp	Digital EVM
sco-websrvmgr	620	tcp	SCO WebServer Manager
sco-websrvmgr	620	udp	SCO WebServer Manager
escp-ip	621	tcp	ESCP
escp-ip	621	udp	ESCP
collaborator	622	tcp	Collaborator
collaborator	622	udp	Collaborator

Serviciu	Număr de port	Protocol	Descriere
aux_bus_shunt	623	tcp	Aux Bus Shunt
aux_bus_shunt	623	udp	Aux Bus Shunt
cryptoadmin	624	tcp	Crypto Admin
cryptoadmin	624	udp	Crypto Admin
dec_dlm	625	tcp	DEC DLM
dec_dlm	625	udp	DEC DLM
asia	626	tcp	ASIA
asia	626	udp	ASIA
passgo-tivoli	627	tcp	PassGo Tivoli
passgo-tivoli	627	udp	PassGo Tivoli
qmqp	628	tcp	QMCP
qmqp	628	udp	QMCP
3com-amp3	629	tcp	3Com AMP3
3com-amp3	629	udp	3Com AMP3
rda	630	tcp	RDA
rda	630	udp	RDA
ipp	631	tcp	IPP (Internet Printing Protocol)
ipp	631	udp	IPP (Internet Printing Protocol)
bmpp	632	tcp	bmpp
bmpp	632	udp	bmpp
servstat	633	tcp	Service Status update (Sterling Software)
servstat	633	udp	Service Status update (Sterling Software)
ginad	634	tcp	ginad
ginad	634	udp	ginad
rlzdbase	635	tcp	RLZ DBase
rlzdbase	635	udp	RLZ DBase
ldaps	636	tcp	protocolul ldap peste TLS/SSL (fost sldap)
ldaps	636	udp	protocolul ldap peste TLS/SSL (fost sldap)
lanserver	637	tcp	lanserver

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
lanserver	637	udp	lanserver
mcns-sec	638	tcp	mcns-sec
mcns-sec	638	udp	mcns-sec
msdp	639	tcp	MSDP
msdp	639	udp	MSDP
entrust-sps	640	tcp	entrust-sps
entrust-sps	640	udp	entrust-sps
repcmd	641	tcp	repcmd
repcmd	641	udp	repcmd
esro-emsdp	642	tcp	ESRO-EMSDP V1.3
esro-emsdp	642	udp	ESRO-EMSDP V1.3
sanity	643	tcp	SANity
sanity	643	udp	SANity
dwr	644	tcp	dwr
dwr	644	udp	dwr
pssc	645	tcp	PSSC
pssc	645	udp	PSSC
ldp	646	tcp	LDP
ldp	646	udp	LDP
dhcp-failover	647	tcp	DHCP Failover
dhcp-failover	647	udp	DHCP Failover
rrp	648	tcp	Registry Registrar Protocol (RRP)
rrp	648	udp	Registry Registrar Protocol (RRP)
aminet	649	tcp	Aminet
aminet	649	udp	Aminet
obex	650	tcp	CBEX
obex	650	udp	OBEX
ieee-mms	651	tcp	IEEE MMS

Serviciu	Număr de port	Protocol	Descriere
ieee-mms	651	udp	IEEE MMS
udlr-dtcp	652	tcp	UDLR_DTCP
udlr-dtcp	652	udp	UDLR_DTCP
repscmd	653	tcp	RepCmd
repscmd	653	udp	RepCmd
aodv	654	tcp	AODV
aodv	654	udp	AODV
tinc	655	tcp	TINC
tinc	655	udp	TINC
spmp	656	tcp	SPMP
spmp	656	udp	SPMP
mdqs	666	tcp	
mdqs	666	udp	
doom	666	tcp	doom Id Software
doom	666	udp	doom Id Software
diclose	667	tcp	campaign contribution disclosures – SDR Technologies
diclose	667	udp	campaign contribution disclosures – SDR Technologies
mecomm	668	tcp	MeComm
mecomm	668	udp	MeComm
meregister	669	tcp	MeRegister
meregister	669	udp	MeRegister
vacdsm-sws	670	tcp	VACDSM-SWS
vacdsm-sws	670	udp	VACDSM-SWS
vacdsm-app	671	tcp	VACDSM-APP
vacdsm-app	671	udp	VACDSM-APP
vpps-qua	672	tcp	VPPS-QUA
vpps-qua	672	udp	VPPS-QUA
cimplex	673	tcp	CIMPLEX

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
cimplex	673	udp	CIMPLEX
acap	674	tcp	ACAP
acap	674	udp	ACAP
dctp	675	tcp	DCTP
dctp	675	udp	DCTP
vpps-via	676	tcp	VPPS Via
vpps-via	676	udp	VPPS Via
vpp	677	tcp	Virtual Presence Protocol
vpp	677	udp	Virtual Presence Protocol
ggf-ncp	678	tcp	GNU Generation Foundation NCP
ggf-ncp	678	udp	GNU Generation Foundation NCP
mrm	679	tcp	MRM
mrm	679	udp	MRM
entrust-aaas	680	tcp	entrust-aaas
entrust-aaas	680	udp	entrust-aaas
entrust-aams	681	tcp	entrust-aams
entrust-aams	681	udp	entrust-aams
xfr	682	tcp	XFR
xfr	682	udp	XFR
corba-iiop	683	tcp	CORBA IIOP
corba-iiop	683	udp	CORBA IIOP
corba-iiop-ssl	684	tcp	CORBA IIOP SSL
corba-iiop-ssl	684	udp	CORBA IIOP SSL
mdc-portmapper	685	tcp	MDC Port Mapper
mdc-portmapper	685	udp	MDC Port Mapper
hwp-wismar	686	tcp	Hardware Control Protocol Wismar
hwp-wismar	686	udp	Hardware Control Protocol Wismar
asipregistry	687	tcp	asipregistry

Serviciu	Număr de port	Protocol	Descriere
asipregistry	687	udp	asipregistry
realm-rusd	688	tcp	REALM-RUSD
realm-rusd	688	udp	REALM-RUSD
elcsd	704	tcp	errlog copy/server daemon
elcsd	704	udp	errlog copy/server daemon
agentx	705	tcp	AgentX
agentx	705	udp	AgentX
borland-dsj	707	tcp	Borland DSJ
borland-dsj	707	udp	Borland DSJ
entrust-kmsh	709	tcp	Entrust Key Management Service Handler
entrust-kmsh	709	udp	Entrust Key Management Service Handler
entrust-ash	710	tcp	Entrust Administration Service Handler
entrust-ash	710	udp	Entrust Administration Service Handler
cisco-tdp	711	tcp	Cisco TDP
cisco-tdp	711	udp	Cisco TDP
netviewdm1	729	tcp	IBM NetView DM/6000 Server/Client
netviewdm1	729	udp	IBM NetView DM/6000 Server/Client
netviewdm2	730	tcp	IBM NetView DM/6000 send/tcp
netviewdm2	730	udp	IBM NetView DM/6000 send/tcp
netviewdm3	731	tcp	IBM NetView DM/6000 receive/tcp
netviewdm3	731	udp	IBM NetView DM/6000 receive/tcp
netgw	741	tcp	netGW
netgw	741	udp	netGW
netrcs	742	tcp	Network based Rev. Cont. Sys.
netrcs	742	udp	Network based Rev. Cont. Sys.
flexlm	744	tcp	Flexible License Manager
flexlm	744	udp	Flexible License Manager
fujitsu-dev	747	tcp	Fujitsu Device Control
fujitsu-dev	747	udp	Fujitsu Device Control

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
ris-cm	748	tcp	Russel Info Sci Calendar Manager
ris-cm	748	udp	Russel Info Sci Calendar Manager
kerberos-adm	749	tcp	kerberos Administration
kerberos-adm	749	udp	kerberos Administration
rfile	750	tcp	
loadav	750	udp	
kerberos-iv	750	udp	kerberos Version iv
pump	751	tcp	
pump	751	udp	
qrh	752	tcp	
qrh	752	udp	
rrh	753	tcp	
rrh	753	udp	
tell	754	tcp	send
tell	754	udp	send
nlogin	758	tcp	
nlogin	758	udp	
con	759	tcp	
con	759	udp	
ns	760	tcp	
ns	760	udp	
rxex	761	tcp	
rxex	761	udp	
quotad	762	tcp	
quotad	762	udp	
cycleserv	763	tcp	
cycleserv	763	udp	
omserv	764	tcp	

Serviciu	Număr de port	Protocol	Descriere
omserv	764	udp	
webster	765	tcp	
webster	765	udp	
phonebook	767	tcp	telefon
phonebook	767	udp	telefon
vid	769	tcp	
vid	769	udp	
cadlock	770	tcp	
cadlock	770	udp	
rtip	771	tcp	
rtip	771	udp	
cycleserv2	772	tcp	
cycleserv2	772	udp	
submit	773	tcp	
notify	773	udp	
rpasswd	774	tcp	
acmaint_dbd	774	udp	
entomb	775	tcp	
acmaint_transd	775	udp	
wpages	776	tcp	
wpages	776	udp	
multiling-http	777	tcp	Multiling HTTP
multiling-http	777	udp	Multiling HTTP
wpgs	780	tcp	
wpgs	780	udp	
concert	786	tcp	Concert
concert	786	udp	Concert
qsc	787	tcp	QSC
qsc	787	udp	QSC

continuare

Tabelul A.1 Continuare

Serviciu	Număr de port	Protocol	Descriere
mdbs_daemon	800	tcp	
mdbs_daemon	800	udp	
device	801	tcp	
device	801	udp	
fcg-udp	810	tcp	FCP
fcg-udp	810	udp	FCP Datagram
itm-mcell-s	828	tcp	itm-mcell-s
itm-mcell-s	828	udp	itm-mcell-s
pkix-3-ca-ra	829	tcp	PKIX-3 CA/RA
pkix-3-ca-ra	829	udp	PKIX-3 CA/RA
rsync	873	tcp	rsync
rsync	873	udp	rsync
iclcnnet-locate	886	tcp	ICL coNETion Locate Server
iclcnnet-locate	886	udp	ICL coNETion Locate Server
iclcnnet_svinfo	887	tcp	ICL coNETion Server Info
iclcnnet_svinfo	887	udp	ICL coNETion Server Info
accessbuilder	888	tcp	AccessBuilder
accessbuilder	888	udp	AccessBuilder
cddb	888	tcp	CD Database Protocol
omginitialrefs	900	tcp	OMG Initial Refs
omginitialrefs	900	udp	OMG Initial Refs
xact-backup	911	tcp	xact-backup
xact-backup	911	udp	xact-backup
ftps-data	989	tcp	protocolul ftp, date, peste TLS/SSL
ftps-data	989	udp	protocolul ftp, date, peste TLS/SSL
ftps	990	tcp	protocolul ftp, control, peste TLS/SSL
ftps	990	udp	protocolul ftp, control, peste TLS/SSL
nas	991	tcp	Netnews Administration System

Serviciu	Număr de port	Protocol	Descriere
nas	991	udp	Netnews Administration System
telnets	992	tcp	protocolul telnet peste TLS/SSL
telnets	992	udp	protocolul telnet peste TLS/SSL
imaps	993	tcp	protocolul imap4 peste TLS/SSL
imaps	993	udp	protocolul imap4 peste TLS/SSL
ircs	994	tcp	protocolul irc peste TLS/SSL
ircs	994	udp	protocolul irc peste TLS/SSL
pop3s	995	tcp	protocolul pop3 peste TLS/SSL (fost spop3)
pop3s	995	udp	protocolul pop3 peste TLS/SSL (fost spop3)
vsinet	996	tcp	vsinet
vsinet	996	udp	vsinet
mairtd	997	tcp	
mairtd	997	udp	
busboy	998	tcp	
puparp	998	udp	
garcon	999	tcp	
applix	999	udp	Applix ac
puprouter	999	tcp	
puprouter	999	udp	
cadlock	1000	tcp	
ock	1000	udp	
surf	1010	tcp	surf
surf	1010	udp	surf
	1023	tcp	Rezervat
	1023	udp	Rezervat

Alte instrumente de securitate pe care le puteți folosi

Această anexă conține legături Web către diverse programe care se pot dovedi utile pentru un administrator de rețea interesat de securitatea rețelei locale. Unele dintre aceste instrumente, dar nu toate, sunt menționate în alte cărți și resurse on-line. Am încercat să localizez sursele din care pot fi descărcate în prezent fiecare dintre aceste instrumente. Câteva dintre sursele pe care le-am verificat anterior includ acum legături invalide. De exemplu, situl Web CERT permitea descărcarea produselor Crack și TCP Wrappers. Aceste pachete nu mai sunt păstrate în arhiva sitului. Dacă descoperiți că una dintre legăturile menționate în această anexă nu mai funcționează, vă rog să faceți două lucruri:

- Folosiți un motor de căutare pentru a încerca să localizați produsele software în altă parte.
- Trimiteți-mi un mesaj e-mail (ogletree@bellsouth.net), astfel încât să pot actualiza edițiile viitoare ale cărții!

Utilitare pentru parole

Așa cum am menționat în capitolul 3, „Securitate și Internet”, una dintre primele linii de apărare pentru orice sistem de calcul este reprezentată de numele de utilizator și parola folosite în procesul de conectare. Din acest motiv, hackerii au dezvoltat multe metode în domeniul descoperirii parolelor. Deoarece mulți utilizatori încă nu iau în serios crearea unor parole greu de ghicit și mulți administratori de sistem nu iau în serios impunerea unor politici bune de alegere a parolelor, în realitate hackerii nu au prea mult de muncă în acest domeniu. Dacă citiți această carte, nu pot decât să presupun că luați în serios acest aspect, așa că primele lucruri pe care le menționează această anexă sunt câteva programe pe care le puteți folosi pentru a îmbunătăți securitatea parolelor. Rețineți că parolele bune sunt o necesitate atât pe gazdele bastion din firewall, cât și pe serverele și stațiile de lucru din rețea.

Crack

Ei bine, dacă este bun pentru hackeri, atunci este bun și pentru mine! Acesta este un program standard de spargere a parolelor, vechi și bun, scris de Alex Muffett, și de mulți ani face probleme administratorilor de sistem. Totuși, la fel ca orice instrument bun, dacă

este folosit în scopuri pozitive, poate fi destul de valoros. Deoarece utilizatorii sunt faimoși pentru folosirea unor parole ușor de ghicit, este logic că ar trebui să folosiți același utilitar pe care îl folosesc și mulți hackeri. Verificați periodic sistemul pentru a descoperi dacă aveți conturi de utilizator ce ar putea permite o pătrundere ușoară.

Puteți descărca utilitarul Crack de pe următorul sit:

<http://www.nomoresecrets.net/download/download.html>

Acest sit pune la dispoziție multe alte instrumente ce pot fi folosite de un administrator interesat de securitate.

Computer Oracle and Password System (COPS)

Pachetul COPS este compus din câteva programe ce pot fi folosite pentru localizarea unor probleme de securitate recunoscute din sistemele UNIX. A fost scris de Dan Farmer, care este unul dintre autorii cărții *How to...by Breaking Into It*.

Puteți descărca pachetul COPS de pe unul dintre următoarele situri:

<http://www.nomoresecrets.net/download/download.html>

sau

<http://ciac.llnl.gov/ciac/ToolsUnixSysMon.html>¹

sau

http://www.auscert.org.au/Information/Tools/other_tools.html

Perl Cops – implementarea în Perl a utilitarului COPS

Acest instrument este asemănător cu COPS, dar este scris în Perl de Steve Romig. Puteți găsi utilitarul Perl Cops la următoarea adresă:

<ftp://coast.cs.purdue.edu/pub/tools/unix/cops-perl.tar>

Tiger

Aceasta este o colecție de scripturi de monitorizare, similară ca funcționare cu COPS. Tiger a fost scris pentru a contribui la îmbunătățirea securității sistemelor Universității A & M din Texas (Texas A & M University), la care aveau acces calculatoare din afara campusului. Puteți găsi pachetul Tiger la adresa:

<http://ciac.llnl.gov/ciac/ToolsUnixSysMon.html>

Pentru Tiger există și o listă poștală. Dacă doriți să vă abonați, trimiteți un mesaj e-mail la următoarea adresă, cu cuvintele subscribe tiger în corpul mesajului:

majordomo@net.tamu.edu

¹ La terminarea traducerii, utilitarele de securitate din acest sit erau disponibile pe pagina <http://ciac.llnl.gov/ciac/SecurityTools.html> (n. trad.)

Instrumente folosite pentru monitorizarea rețelei

Utilitarele din această secțiune se referă la rețea. Unele, cum ar fi ARGUS, pot fi folosite pentru monitorizarea traficului IP în rețea, în timp ce altele, precum SWATCH, sunt folosite pentru gestionarea fișierelor jurnal, astfel încât să urmărești ce se întâmplă în rețea.

ARGUS

Acesta este un instrument de auditare IP, scris de Carter Bullard și Chas DeFatta, și poate fi folosit pentru a analiza tranzacțiile IP.

Puteți descărca utilitarul ARGUS de pe următoarele situri:

<ftp://ftp.sei.cmu.edu/pub/argus>

sau

http://www.auscert.org.au/Information/Tools/other_tools.html

Simple WATCHer (SWATCH)

SWATCH este un utilitar scris de Stephen Hansen și Todd Atkins și poate fi folosit pentru simplificarea operațiilor de gestionare a fișierelor jurnal. SWATCH poate să filtreze anumite evenimente și să execute diferite acțiuni în funcție de ceea ce găsește. Poate fi folosit pentru a elimina din fișier înregistrările obișnuite, care nu fac decât să ocupe spațiu.

Puteți descărca utilitarul SWATCH de pe următorul sit:

<ftp://ftp.stanford.edu/general/security-tools/swatch>

Internet Security Scanner (ISS)

ISS, scris de Cristopher Klaus, poate fi folosit pentru a sonda una sau mai multe adrese IP, în căutarea unor probleme de securitate recunoscute.

Puteți descărca utilitarul ISS de pe următoarele situri:

<ftp://ftp.iss.net/pub/iss/>

sau

<http://www.nomoresecrets.net/download/download.html>

Security Administrator Tool for Analyzing Networks (SATAN)

Acest instrument a fost amintit în capitolul 12, „Instrumente pentru firewall-uri disponibile în Internet”. Este menționat din nou aici, în caz că ați sărit peste capitolul respectiv. Deși trebuie să aveți cunoștințe avansate privind administrarea sistemelor UNIX și lucrul în rețele TCP/IP ca să configurați utilitarul și să obțineți avantaje în urma folosirii acestuia, SATAN este un instrument configurabil excelent.

Puteți găsi utilitarul SATAN la următoarele adrese:

<http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html>

sau

<http://www.nomoresecrets.net/download/download.html>

Courtney – vă urmărește SATAN?

Deoarece SATAN poate fi folosit pentru investigarea punctelor vulnerabile ale rețelei, deseori este folosit nu numai de administratori de rețea respectabili, ci și de persoane mai puțin respectabile, care doresc să vă facă o mulțime de probleme. Desigur, este vorba din nou de hackeri. Utilitarul Courtney poate fi folosit pentru monitorizarea rețelei, pentru a vedea dacă utilitarul SATAN este folosit împotriva dumneavoastră și pentru a încerca să identificați sursa scanării.

Puteți descărca utilitarul Courtney de pe următoarele situri:

<http://ciac.llnl.gov/ciac/ToolsUnixNetMon.html>

sau

http://www.auscert.org.au/Information/Tools/other_tools.html

Gabriel – un alt luptător împotriva lui SATAN

Acesta este un alt instrument care, ca și Courtney, poate fi folosit pentru a determina dacă utilitarul SATAN vă sondează rețeaua.

Puteți descărca utilitarul Gabriel de pe următorul sit:

<http://ciac.llnl.gov/pub/ciac/ToolsUnixNetMon.html>

Merlin – utilitar de interfață

Merlin nu este un instrument de securitate în sine, dar oferă o interfață grafică cu utilizatorul pentru cele mai populare instrumente, cum ar fi SATAN, COPS și TripWire.

Puteți descărca utilitarul Merlin de pe următorul sit:

<ftp://ciac.llnl.gov/ciac/sectools/unix/merlin/merlin.tar.gz>

ifstatus – localizarea interfețelor de rețea care lucrează în modul eterogen

Atunci când rulează în modul eterogen¹, un adaptor de rețea transmite toate pachetele de pe cablu în sus prin stiva de protocoale. De fapt, acesta este modul de lucru folosit de un dispozitiv de interceptare² Ethernet pentru a captura tot traficul de rețea în vederea analizei. De asemenea, poate fi folosit de cineva care ascultă rețeaua și care poate

¹ În original, *promiscuous mode*, numit uneori și *mod promiscuu* (n. trad.)

² În original, *sniffer* (n. trad.)

intercepta parole și alte date importante. Folosiți `ifstatus`, scris de Dave Curry, pentru a localiza adaptoarele de rețea care operează în acest mod în rețeaua dumneavoastră.

Puteți descărca utilitarul `ifstatus` de pe următorul sit:

<ftp://coast.cs.purdue.edu/pub/tools/unix/ifstatus/ifstatus.tar.Z>

NID – Network Intrusion Detector

Acest utilitar, produs de Computer Security Technology Center, este compus din mai multe instrumente care pot detecta intruziunile în rețea. De asemenea, poate fi folosit pentru a determina dacă utilizatori valizi încearcă să facă lucruri care nu le sunt permise:

Puteți descărca utilitarul NID de pe următorul sit:

<http://ciac.llnl.gov/ciac/ToolsUnixNetMon.html>

tcpdump

Acest utilitar a fost scris de Van Jacobson și poate fi folosit cu un adaptor Ethernet ce lucrează în modul eterogen pentru capturarea și examinarea pachetelor din rețea. Posibilitățile de filtrare vă ajută să îngustați domeniul de căutare. Pentru cei care nu își pot permite un analizor de protocoale de rețea performant (a se citi scump), aceasta poate fi o alternativă destul de bună.

Puteți descărca utilitarul `tcpdump` de pe următorul sit:

<http://ciac.llnl.gov/ciac/ToolsUnixGeneral.html>

Instrumente de verificare a stării sistemului

Programele din această secțiune pot fi folosite pentru a verifica dacă sistemul dumneavoastră are breșe de securitate evidente.

Secure_Sun

Acest program a fost scris de David Safford și poate fi folosit pentru verificarea mai multor tipuri de mașini SunOS privind existența unor probleme de securitate cunoscute.

Puteți descărca utilitarul `Secure_Sun` de pe următorul sit:

http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html

trojan.pl

Acesta este un program care examinează toate fișierele executabile din calea de căutare, verificând dacă există eventuale programe de tip cal troian ce ar putea fi executate de root.

Acest program poate fi descărcat de pe următorul sit:

<http://www.cerias.purdue.edu/coast/archive/data/categ50.html>

Tripwire

Acest utilitar poate fi folosit pentru a menține integritatea sistemelor dumneavoastră de fișiere. Tripwire stochează informații despre fișiere și directoare într-o bază de date, astfel încât să puteți descoperi, printr-o scanare ulterioară, dacă fișiere de sistem importante au fost modificate.

Puteți descărca utilitarul Tripwire de pe următoarele situri:

<http://www.tripwiresecurity.com/>

sau

<ftp://info.cert.org/pub/tools/tripwire/>

MD5

MD5 poate fi folosit pentru producerea unui rezumat de 128 de biți al fișierelor din sistemul dumneavoastră. Comparând rezultatul curent cu „amprente” produse la scanările anterioare, puteți să determinați dacă au fost modificate fișiere de sistem importante.

Pentru mai multe informații despre MD5, puteți consulta documentul RFC 1321.

Puteți descărca utilitarul MD5 de pe următorul sit:

<ftp://info.cert.org/pub/tools/md5/>

lsf (List Open Files)

Acest mic utilitar, scris de Vic Abell, poate fi folosit pentru a afișa fișierele deschise pe un sistem UNIX, împreună cu procesele care le-au deschis.

Puteți descărca utilitarul `lsf` de pe următorul sit:

<ftp://vic.cc.purdue.edu/pub/tools/unix/lsf/>

Variante de înlocuire pentru programe populare

Multe comenzi UNIX conțin erori sau au alte probleme ce pot fi folosite în dezavantajul dumneavoastră. Pentru unele dintre acestea sunt disponibile programe de înlocuire sau de corectare.

smrsh – sendmail Restricted Shell

Scris de autorul programului `sendmail`, `smrsh` vă ajută să vă protejați împotriva unora dintre problemele cauzate de acest program de 20.000 de linii de cod. Utilitarul este inclus în pachetul `sendmail` începând cu versiunea 8.7.1 (și poate fi găsit în subdirectorul `/smrsh`). Rețineți că `smrsh` nu corectează toate problemele din `sendmail`, dar dacă folosiți o versiune foarte veche, ar putea fi o idee bună să treceți la cea mai nouă versiune.

Puteți descărca utilitarul smrsh de pe următorul sit:

<ftp://ftp.uu.net/pub/security/smrsh/>

fingerd* – înlocuitor pentru programul *finger

Scrisă de Mike Shanzer, această versiune a comenzii *finger* asigură în plus liste privind conectarea și liste pentru controlul accesului.

Acest program poate fi descărcat de pe următorul sit:

http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html

sfingerd* – un alt înlocuitor pentru programul *finger

Acesta este un program *finger* mic și sigur, scris de Laurent De-mailly.

Și acest program poate fi descărcat de pe următorul sit:

http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html

PortMap V3

Scris de Wietse Venema, autorul setului de instrumente TCP Wrappers, acesta este un înlocuitor pentru programul de mapare a porturilor. Include metode pentru controlul accesului, asemănătoare cu cele folosite de TCP Wrappers.

Puteți descărca acest program de pe următorul sit:

http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html

SRA – autentificare RPC sigură pentru Telnet și FTP

Acest utilitar provine de la Universitatea A & M din Texas și asigură autentificarea sigură, criptată prin rețea pentru Telnet și FTP, care, în mod normal, transmit parolele sub formă de text clar.

Acest utilitar poate fi descărcat de pe următorul sit:

http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html

Authd – demon server pentru autentificare

Documentul RFC 931 descrie un demon server ce poate fi folosit pentru a furniza un nume de utilizator pentru conexiunile prin rețea. Dacă un sistem este compatibil cu specificațiile RFC 931, sistemele de la distanță pot interoga demonul server pentru a afla cine folosește de fapt conexiunea prin rețea. În acest fel poate fi sporită securitatea, deoarece informațiile pot fi înregistrate în fișiere jurnal sau pot fi folosite de programe pentru controlul accesului.

Utilitarul Authd poate fi descărcat de pe următorul sit:

http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html

***su* – program *su* fals**

Dacă un hacker folosește programul *su* pentru a obține informații despre utilizatorii din sistemul dumneavoastră, păcăliți-l cu această versiune falsificată a programului, care în loc să ofere informații reale, vă avertizează că este folosit. Acest program a fost scris de Shawn F. McKay.

Acest program poate fi descărcat de pe următorul sit:

http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html

***ssh* – pachetul Secure Shell**

Deși multă lume știe că instrumentele de tip *r** (cum ar fi *rsh* și *rlogin*) prezintă o problemă de securitate în rețea, este greu să renunțați la ele după ce utilizatorii s-au obișnuit cu folosirea lor. Utilitarele din pachetul *ssh* adaugă la aceste instrumente metode puternice de criptare și autentificare, astfel încât puteți continua să oferiți utilizatorilor comoditate în folosire și funcționalitate.

Puteți descărca pachetul *ssh* de pe următorul sit:

<ftp://ftp.cs.hut.fi/pub/ssh/>

Resurse suplimentare

Nici o carte nu ar putea conține toate informațiile de care aveți nevoie pentru configurarea unui firewall bun, cu atât mai puțin pentru întreținerea acestuia. Unul dintre motive este faptul că Internetul se extinde rapid și sunt dezvoltate continuu noi protocoale și servicii. Trebuie să cunoașteți aceste noi dezvoltări pentru a putea determina dacă firewall-ul dumneavoastră este corect configurat pentru a le face față. Un alt motiv pentru care aveți nevoie de resurse suplimentare este faptul că aplicațiile, protocoalele și sistemele de operare nu sunt perfecte. Mereu sunt descoperite noi erori și breșe de securitate. Dacă nu știți că aveți o breșă de securitate în firewall, este evident că nu veți fi protejați!

Această anexă indică mai multe adrese pe care le puteți vizita pentru a obține informații suplimentare despre subiectele discutate în cartea de față, precum și adrese pe care le puteți folosi pentru a vă menține în actualitate în privința problemelor de securitate, pe măsură ce acestea sunt descoperite. Și în acest caz, deoarece Internetul se extinde și se modifică în fiecare zi, s-ar putea să descoperiți în această anexă adrese URL care nu mai sunt valabile. Acesta este prețul pe care îl plătiți pentru progres! Dacă nu reușiți să localizați o resursă menționată aici după adresa URL specificată, încercați să folosiți un motor de căutare bun (cum ar fi www.altavista.com) pentru a vedea dacă resursa este încă disponibilă, folosind o altă adresă URL.

Această anexă nu conține lista furnizorilor de produse pentru firewall-uri, deoarece nu am posibilitatea să evaluez fiecare produs și să îi determin utilitatea. Ultimul lucru pe care aș vrea să îl fac este să vă spun ce produs să cumpărați. Nici un autor nu poate face acest lucru, deoarece autorii nu știu nimic despre rețeaua dumneavoastră și trebuie să stabiliți de ce aveți nevoie în funcție de ceea ce aveți deja. În schimb, veți găsi aici situri dedicate problemelor de securitate și le puteți folosi pentru a vă instrui.

În caz că nu v-ați dat încă seama de acest lucru, ar trebui să luați în considerare și posibilitatea de a vizita pagina de bază a furnizorului sistemului de operare sau aplicației pe care o folosiți. Furnizorul vă poate pune la dispoziție informații importante și, probabil, programe de corectare sau alte modalități ce pot fi folosite pentru rezolvarea problemelor pe care le-ați descoperit.

www.first.org Forum of Incident Response and Security Teams

Această organizație include membri ai echipelor de răspuns la incidente din situri academice, comerciale și guvernamentale. În acest sit veți găsi multe documente referitoare la probleme de securitate. În plus, aici puteți găsi adrese ale unor liste poștale

rezervate membrilor. Dacă nu doriți să deveniți membru al organizației FIRST, puteți să vă abonați la lista poștală publică, folosită pentru discuții referitoare la probleme de securitate, precum și pentru publicarea noilor sugestii privind securitatea.

Pentru a vă abona, trimiteți un mesaj e-mail cu conținutul „subscribe first-info” la adresa first-majordomo@first.org.

www.sans.org/giac.htm Institutul SANS

Institutul SANS (Systems Administration, Networking, and Security) este o organizație care cuprinde peste 62.000 de profesioniști ce lucrează ca administratori de rețea, de securitate sau de sistem. Organizația întreține un sit Web care vă poate ajuta să găsiți informații actualizate despre programe cu comportament nedorit și despre instrumente pe care le puteți folosi pentru a îmbunătăți securitatea sitului dumneavoastră. Centrul de analiză a incidentelor globale (GIAC – Global Incident Analysis Center) al acestei organizații urmărește breșele de securitate și metodele ce pot fi folosite pentru închiderea acestora. Dacă sunteți în căutarea unui nou loc de muncă, puteți consulta aici și o listă de salarizare.

Pe lângă prezența în Web, SANS oferă cursuri de instruire, care vă pot fi de ajutor dumneavoastră sau altor membri ai sitului dumneavoastră, și diferite instrumente și resurse ce pot fi folosite pentru a vă îmbunătăți securitatea. De asemenea, în fiecare an are loc o conferință SANS care, de obicei, durează o săptămână. În plus, SANS găzduiește o întrunire mai restrânsă, numită SANS SNAP. SNAP este acronimul pentru System and Network Assurance Program (program de asigurare a rețelelor și sistemelor) și reprezintă o serie de cursuri de mai multe zile referitoare la probleme de securitate.

www.cert.org Centrul de coordonare CERT

Această adresă URL vă duce la situl Web CERT (Computer Emergency Response Team). Această organizație, având sediul la Institutul de Inginerie Software din cadrul Universității Carnegie-Mellon (Carnegie-Mellon University's Software Engineering Institute), elaborează sugestii privind formele noi de atac descoperite și este unul dintre cele mai bune situri dedicate acestui scop. Organizația CERT a fost creată după ce virusul Internet Worm a făcut dezastru în Internet în 1988. În acest sit puteți să vă înscrieți în lista poștală a organizației, ceea ce vă poate ajuta să rămâneți la curent cu problemele de securitate referitoare la Internet.

În întreaga lume există alte câteva situri care folosesc numele CERT. Puteți să le vizitați pentru a compara sugestiile, instruirea și alte resurse oferite:

- www.cerias.purdue.edu/pcert/pcert.html – Organizația PCERT (Purdue Computer Emergency Response Team) are ca sediu, așa cum probabil bănuți, Universitatea Purdue.
- www.nic.surfnet.nu/surfnet/security/cert-nl.html – Acest sit (aflat în Olanda) face parte din organizația Global Forum of Incident Response and Security Teams.

- www.cert.dfn.de/eng – Această pagină Web reprezintă organizația CERT din Germania. Situl conține puține pagini în engleză, dar poate fi o resursă utilă pentru toți germanii minunați care au cumpărat această cartel!
- www.cert.lu – Această pagină Web reprezintă organizația CERT din Luxemburg.
- www.cert.au – Această pagină Web reprezintă organizația CERT din Australia.
- www.afcert.csap.af.mil – AFCERT (Air Force Computer Emergency Response Team) este organizația CERT a Forțelor Aeriene ale Statelor Unite, având sediul în Baza Aeriană Kelly.
- www.infosec.nosc.mil/infosec.html – Un al sit militar din Statele Unite, aceasta fiind adresa URL a paginii Web întreținute de organizația CERT a Forțelor Navale ale Statelor Unite.

De asemenea, dacă se întâmplă să descoperiți o nouă formă de atac, nu uitați să folosiți situl CERT pentru a trimite un raport, astfel încât și alții să poată fi informați!

www.microsoft.com

Fără îndoială, ați auzit în ultimii ani despre multe rapoarte privind descoperirea unor hibe sau a altor probleme de securitate ale sistemelor de operare (Windows 98, Windows NT și Windows 2000) și ale aplicațiilor (Internet Explorer, de exemplu) produse de Microsoft. Dacă folosiți produsele acestei companii, puteți fi sigur că Microsoft încearcă să păstreze controlul și, dacă vreți să faceți același lucru, puteți să vizitați situl companiei și să vă înscrieți în lista poștală pentru securitate. Pentru a vă abona, vizitați situl www.microsoft.com și executați clic pe butonul Subscribe de pe bara cu instrumente din partea de sus a paginii Web. Introduceți informațiile necesare și veți începe să primiți periodic mesaje e-mail.

De asemenea, ar trebui să vizitați adresa www.microsoft.com/security, unde este o pagină Web pe care Microsoft a dedicat-o problemelor de securitate. De aici puteți descărca ultimele actualizări ale produselor Microsoft și puteți obține mai multe informații despre produse specifice.

www.securityportal.com

Aceasta este pagina Web a unui furnizor de servicii Internet, care oferă și o mulțime de informații despre probleme de securitate legate de Internet. Puteți vizita această pagină pentru a vă înscrie în lista poștală Security Portal Weekly Newsletter. Deși este un sit comercial, pune la dispoziție și un forum de discuții și știri despre ultimele evenimente legate de securitate.

www.ntsecurity.net

Acest sit, așa cum probabil bănuieți, este dedicat problemelor de securitate legate de sistemul de operare Windows NT (acum Windows 2000) și produsele înrudite. Este sponsorizat de revista *Windows 2000 Magazine* (numită anterior *Windows NT Magazine*,

publicată de Duke Communications International Inc.). Dacă folosiți produse Windows, ar trebui să luați în considerare vizitarea acestui sit, deoarece conține un număr mare de resurse și, desigur, o listă poștală de e-mail în care vă puteți înscrie. De asemenea, dacă folosiți sistemele de operare Windows, autorul vă recomandă călduros să vă abonați și la revistă, deoarece este, probabil, una dintre cele mai bune publicații actuale despre Windows.

www.l0pht.com

Acest sit Web este pagina de bază a organizației L0pht Heavy Industries. În momentul scrierii cărții de față, această organizație de hackeri (?) tocmai își unise forțele cu o nouă firmă, numită @Stake. Ce rezultă atunci când o companie orientată spre probleme de securitate își unește forțele cu un grup de hackeri? Ei bine, după cum indică știrile din ultimii ani, băieții de la L0pht sunt foarte buni în descoperirea viciilor de securitate ale sistemelor de operare importante. Combinându-și forțele cu o companie specializată în probleme de securitate, cine știe care va fi rezultatul? Oricum, nu uitați să vizitați acest sit Web, pentru a profita de volumul mare de resurse puse la dispoziție.

Lista poștală pentru firewall-uri

Aceasta este o listă poștală cu mai multe componente. Dacă aveți întrebări, vreți să dați răspunsuri sau vreți doar să țineți pasul cu noile aspecte legate de firewall-uri, arhitectura acestora și alte probleme de securitate, ar trebui să vă abonați la această listă poștală.

Pentru a vă înscrie în lista poștală, trimiteți comanda subscribe firewalls în corpul unui mesaj e-mail (nu în linia „Subject:”) către următoarea adresă:

majordomo@greatcircle.com

Dacă nu doriți să vedeți fiecare mesaj în parte, este disponibil și un rezumat. Pentru a vă abona la acest rezumat, trimiteți comanda subscribe firewalls-digest în corpul unui mesaj e-mail către aceeași adresă.

De asemenea, aveți acces la arhivele listei poștale și la alte materiale utile, folosind următoarea adresă URL:

<ftp://ftp.greatcircle.com/pub/firewalls/index.html>

<http://waldo.wi.mit.edu/WWW/tools/security/www-security-faq/index.html>

La această adresă URL puteți găsi lista World Wide Web Security FAQ, cu întrebări adresate frecvent. Dacă operați un server Web, această listă FAQ v-ar putea fi de ajutor în timpul configurării.

¹ Ediția originală în limba engleză, apărută în iunie 2000 (n. trad.)

www.cerias.purdue.edu/coast Computer Operations, Audit and Security Technology (COAST)

Acest sit Web este gestionat de departamentul de informatică (Computer Sciences Department) al Universității Purdue. Aici veți găsi o listă poștală de informare și diferite rapoarte și articole referitoare la securitatea calculatoarelor. Arhiva COAST conține o cantitate mare de informații, de la rapoarte oficiale și instrumente software la legături către alte situri de securitate.

ciac.llnl.gov Computer Incident Advisory Capability

Situl Web al Departamentului Energiei din Statele Unite este găzduit de Computer Security Technology Center for Lawrence Livermore National Laboratory. Deși servește ca punct central de diseminare a informațiilor despre noile probleme de securitate, veți găsi aici și multe alte resurse, inclusiv o bază de date cu viruși și o listă de false probleme – amenințări de securitate care de fapt nu există!

Câteva dintre utilitățile de securitate menționate în anexa B, „Alte instrumente de securitate pe care le puteți folosi”, pot fi descărcate de pe acest sit.

www.fedcirc.gov Federal Computer Incidence Response Capability

Un alt sit Web guvernamental în care puteți găsi o varietate de resurse legate de securitatea rețelor și calculatoarelor. De asemenea, de pe acest sit puteți descărca multe dintre utilitățile menționate în anexa B, cum ar fi ISS, SATAN și COPS. Un document foarte bun pe care îl puteți obține de pe acest sit este „Metode de protejare a mijloacelor informaționale critice”¹, scris de Critical Infrastructure Assurance. Acest document oferă o imagine generală asupra securității rețelor, de la viruși informatici la aspecte de securitate fizică. Deși a fost elaborat pentru agențiile federale din Statele Unite, poate fi un instrument excelent pentru instruirea colaboratorilor, și în special a șefilor, privind necesitatea păstrării unei bune securități a rețelei.

www.nsi.org/compsec.html The National Security Institute's Security Resource Net

Acesta este un alt sit Web bun pe care îl puteți folosi pentru a descărca articole și instrumente de securitate. De pe acest sit puteți comanda diferite materiale documentare elaborate de CSI (Computer Security Institute), care acoperă anumite domenii de

securitate, cum ar fi prevenirea virusărilor și aspecte legate de securitatea poștei electronice. Acestea nu sunt ieftine, dar informațiile conținute merită prețul.

xforce.iss.net/maillists/otherlists.php3

Acest sit conține o foarte bună listă de liste poștale legate de securitatea rețelor și calculatoarelor. Pentru fiecare listă găsiți o scurtă descriere și instrucțiuni de înscriere.

¹ „Practices For Securing Critical Information Assets” (n. trad.)

Index

Simboluri

! (semnul exclamării), 232
(diez), 154, 225
%%, variabilă, 214
- (cratimă), 226
- (punct), 49
/ (diagonală la dreapta), 269
3DES, 167
: (două puncte), 225, 269
?, comandă, 233

A

-A *direcție*, parametru, 260
-a *politică*, comandă, 260
-a *port*, parametru în linia de comandă, 253
-A *regulă de înlănțuire*, comandă, 268
A, tip de înregistrare, 53
%A, variabilă, 214
AAAA, tip de înregistrare, 53
abonarea la liste poștale
 Firewalls, 375
 SOCKS, 247-248
accept, cuvânt cheie, 266
accept, tintă, 266
Access the Internet Using a Proxy Server, casetă de validare, 286-287
access.log, fișier, 254
accesul la fișiere criptate (PGP), 192
ACK Flag, câmp, 64
ACK, bit, 106
activarea auditării evenimentelor, 160-161
acțiuni, 152-153
adăugarea cheilor publice la inelele cu chei, 191
Add Email ID, buton, 292-293
Add or Remove User Services, buton, 297
Add Users and Groups, casetă de dialog, 127, 160-161, 281
Address Mask Reply, tip de mesaje, 34
Address Mask Request, tip de mesaje, 34
Address Resolution Protocol. *Vezi* ARP
Address Type, câmp, 246

Administrative Tools, comandă (meniul Programs), 158
Administrative Tools, comenzi de meniu
 Event Viewer, 162-163
 User Manager, 158
Administrative Tools, dosar, 158
adresare IP, 32
adresă de difuzare pe grupuri, 39, 314
adresă unică (unicast), adrese, 39, 314
adrese
 bucă, 39
 calcularea subrețelelor, 42
 cu destinație unică (unicast), 39, 314
 difuzare, 39
 difuzare pe grupuri (multicast), 39
 fizice, 35
 hardware, 32, 35
 IP, 32-35
 alocare, 303
 clase. *Vezi* *adrese IP*, *clase lungime*, 35
 specificare, 268-269
 translatare, 32
 IPv6, 314
 împărțire (măști de subrețea), 41
 MAC, 32-35
 notația zecimală cu punct, 35-36
 rețele private, 39
 specificare, 269
adrese de difuzare, 39
adrese de subrețea, calculare, 42
adrese fizice, 35
adrese hardware, translatate, 32, 35
adrese sursă (SA), 181
Advanced, comandă (meniul Category), 256
Advanced, comenzi de meniu (Proxies), 256
AH (Authentication Header), 180, 182-184
alarmare prin email, configurare, 286
alarme, 285-286
alegerea serverelor (SQUID), 251
Alerting, etichetă, 286
algoritmii criptografici, 181

ALL, cuvânt cheie, 213
alocarea adreselor IP, 303
alocarea adreselor statice, 140
alocarea dinamică a adreselor, 140
alocarea soclurilor, 242-243
altavista, sit Web, 372
anonim, FTP, 48
antet de extensie pentru autentificare, 312-313
antet de extensie pentru încapsularea informațiilor de securitate, 312-313
antet de extensie pentru rutare, 312-314
antet de extensie salt-cu-salt, 312-313
antet pentru cereri (UDP), 246
antet TCP, 64
anteturi
 extensie (IPv6), 312-314
 IP, 43-45
 IP, informații de antet, 100-101
 lungime fixă (IPv6), 309-312
 TCP, 64
 TCP, informații de antet, 101-103
 UDP, informații de antet, 103-104
anteturi cu lungime fixă (IPv6), 309-312
anteturi de extensie (IPv6), 312-314
anteturi de pachete, 13-14
anycast, tip de adresă, 314
apeluri, interceptare (funcții de rețea WinSock), 241, 247
aplicație de gestionare (CommandView Firewall), 364/365
aplicație, strat OSI, 27, 30
aplicații, 226
 „SOCKSificarea” aplicațiilor, 202, 247
 intermediar, 245
 netatcl, 223
 ștergerea fișierelor inutile de pe gazdele bastion, 120-121
aplicații intermediar, 245
Application, fișier jurnal pentru evenimente, 161
Argus, 366
Argus, sit Web, 366
arhitectură (firewall-uri), 81

arhitectură bazată pe subrețele ecranate
 subrețele ecranate multiple, 89-92
 zonă demilitarizată (DMZ), creare, 88-90
ARP (Address Resolution Protocol), protocol, 26-27, 32-33
arp, comandă, 33
ARP, metodă de difuzare, 33
ARP, tabel, 33
arpa, domeniu organizațional, 50
Array, buton, 280-281
ASCII Armor, 192
asigurarea conexiunilor sigure, 73
asistență tehnică
 adresare IPv6, 245
 autentificare, 245
 NAT, 303
 nume de domenii, 245
 SOCKS, 247-248
asociații de securitate, 180-182
atacuri distribuite prin interdicerea unui serviciu, 66-68
atacuri prin interdicerea unui serviciu, 63
 blocarea calculatoarelor gazdă, 63
 distribuite, 66-68
 prevenire, 63
 reconfigurarea informațiilor despre gazde/rețele, 63
 supraîncărcarea resurselor limitate, 63
Attach to Firewall, comandă (meniul Command View File), 294
attribute listă_de_valori, 225
Audit Policy, casetă de dialog, 158-161
Audit These Events, buton radio, 158
Audit, comandă (meniul Policy), 158
auditare, 148, 151, 164
 conectări executate cu succes, 150
 eșecuri la conectare, 150
 gazde bastion, configurare, 128
 IP (Argus), 366
 syslog (utilitar UNIX), 181-182.
 Vezi și *syslog*, fișier de configurare
 utilizarea imprimantei, 161
Windows NT, 157-158
 configurarea evenimentelor ce vor fi auditate. *Vezi* *evenimente*, *auditare*
 dezactivare, 159
 Event Viewer, 157

auditare. *Vezi* și *fișiere jurnal*;
 înregistrare în jurnal
Auditing, buton, 160-161
autentificare, 166, 307
 asigurarea suportului, 245
 GSS-API, 246
 VPN, 176-177
autentificarea utilizatorilor, 59-60
 -auth, opțiune, 232
authd, 201, 220, 239, 370
Authd, sit Web, 370
Authentication Data, câmp, 183
Authentication Header (AH), 180, 182-184
Authentication Server Daemon (authd), program de corectare, 370
Authentication Server Protocol, 215
authserver gazdă port, cuvânt cheie, 228
Auto Dial, buton, 280
AutoDial, 280
automatizare
 operații UNIX, 156
 revizuirea fișierelor jurnal, 150

B

-b, opțiune în linia de comandă, 262, 263
badadmin utilizator, comandă, 235
baddir director, comandă, 235
bază de date centralizată cu utilizatori, 60
baze de date
 conectare, 59-60
 parole, 59-60
 SAM (Security Accounts Manager), 59-60
 utilizatori (centralizate), 60
baze de date pentru parole, 59-60
baze de date, fișiere, 52
BIND (Berkeley Internet Name Domain), 53. *Vezi* și *DNS*
BIND Request, câmp, 244, 246
blocarea accesului la Internet, 144-145
blocarea calculatoarelor gazdă (atacuri prin interdicerea unui serviciu), 63
Blowfish, 168
Blowfish, sit Web, 168
bootp, protocol, 35
BSDI (BSD/OS), 301
bucă, adresă, 39
buletine (CIAC-2319), 67
buletine de informare, căutare, 67
buletine informative referitoare la securitate, 61-62, 93-94

butoane
 Add Email ID, 292-293
 Add or Remove User Services, 297
 Array, 280-281
 Auditing, 160-161
 Auto Dial, 280
 Cache Filters, 283
 Certificates, 173-174
 Client Configuration, 281
 LAN Settings, 256
 Local Address Table
 Plugs, 280-281
 Search, 161
 Security, 278
 Server Backup, 281
 Server Restore, 281
 Show Users, 161, 281
 View, 256

C

-c, comandă, 261
%c, variabilă, 214
CA (Certificate Authority), 171, 181
cache de proprietăți, gestionare, 282-284
Cache Filters, buton, 283
cache, fișier, 52
cache.log, fișier, 254
Caching, pagină de proprietăți, 282-283
cal troieni, 24, 68-70
calculare
 subrețele, adrese, 42
 valorii pentru subrețea, 41
calcularea subrețelelor, 41
calculatoare
 gazdă, blocare (atacuri prin interdicerea unui serviciu), 63
 securitate fizică, 61
calculatoare gazdă, blocare (atacuri prin interdicerea unui serviciu), 63
Caldera, sit Web, 259
canale sigure, creare, 175
capacitate de apelare și primire a apelurilor, 156
casete de dialog
 Add Users and Groups, 127, 160-161, 281
 Audit Policy, 158-161
 Certificates, 173-174
 Configure Mail Alerting, 286
 Create Email Rule, 292-293
 Directory Auditing, 160-161
 Directory Permissions (Windows NT), 127-129
 Event Log Settings, 163
 Installation Options (Microsoft Proxy Server, configurare), 274

Internet Options, 256
Join Array, 280-281
Key Generation Wizard, 194
Local Area Network (LAN)
Settings, 146-147, 256
Proxy Settings, 146, 256,
286-287
Security, 286
Select Components, 193
Select Program Folder, 291
Select User Service for Master
Security Plan, 297
Service (Windows NT), 119
Set Notification Command,
292-293
Setup Complete, 291
Setup Type, 290
Special Directory Access
(Windows NT), 128

casete de validare
Access the internet Using a Proxy
Server, 286-287
Enable Caching, 282
Enable Dynamic Packet Filtering
on Microsoft Proxy Server
Packets, 278
Enable E-Mail Notification,
292-293
Enable Logging Using, 285
Enable Packet Filtering on
External Interface, 278
Enable Web Publishing, 284
Failure, 158
Replace Auditing on Existing
Files, 160-161
Replace Auditing on
Subdirectories, 160-161
Send SMTP Mail, 286
Success, 158

Category, blocare, 144
Category, meniu (Advanced), 256
căi pentru cereri, 284
căutare inversă a numelor, 218
câmpuri
/etc/inetd, fișier de configurare,
211
/etc/inetd.conf, fișier, 221-222
ACK Flag, 64
Address Type, 246
antet de lungime fixă (IPv6),
310-312
anteturi IP
Datagram Length, 44
Destination Address, 44
Flags, 44
Fragment Offset, 44
Header Checksum, 44
Identification, 44
Internet Header Length (IHL),
43
Options, 45
Padding, 45
protejare, 182-183
Protocol, 44
Source Address, 44
Time to Live (TTL), 44
Type of Service (TOS), 43
Version, 43
BIND Request, 244, 246
Change Settings, 163
Class, 55
cod de răspuns (număr de
versiune), 242-243
CONNECT Request, 242, 246
Data Type, 211, 221
Destination Address, 246,
312-313
Destination Port, 246
Domain Name, 54
Don't Fragment (DF), 44
Email Address, 54
Expire Rate, 54
FIN Flag, 64
Flags, 68
Flow Label, 312
Fragment Offset, 68
Hop Limit, 312
Identification, 68
IN, 53-55
Maximum Log Size, 163
Maximum TTL, 54
Name, 211, 221
Next Header, 312
Payload Length, 312
Port, 256
Primary Server, 54
Process arguments, 211, 222
Protocol, 211, 221
Proxy Address to Use, 256
Refresh Rate, 54
Retry Rate, 54
Sequence Number, 64
Serial Number, 54
Server, 211, 222
SOA, 53
SOA, înregistrări, 53-54
Source Address, 73, 312-313
SYN Flag, 64
Traffic Class, 312
UDP ASSOCIATE Request
(SOCKS V5 Command Code),
246
UID, 211, 221
Version, 312
Version Number, 246
Wait-state, 211, 221
**câmpuri din antet (IP), protejare,
182-183**
cereri
BIND, 244
CONNECT (SOCKS V4), 242
cereri ale clienților, manevrare, 284

CERN, format standard, 255
CERT (Computer Emergency
Response Team), 373-374
CERT Coordination Center, sit
Web, 373-374
certIFICATE
digitale, 181
emitere, 172
**Certificate Authority (CA), 171,
181**
certificate digitale, 171-172, 181
Certificate Path, etichetă, 173-174
**Certificate, casetă de dialog,
173-174**
Certificates, buton, 173-174
CH (CHAOS), clasă, 55
Change Settings, câmp, 163
**Check Alive, comandă
(CommandView Firewall), 296**
chei, 167
decriptare, 169
denumire, 190
publice, 191
schimb, 168, 181
stocare, 190-191
chei publice, 191
**cheie publică (asimetrică),
criptare, 66, 201-203, 228. Vezi și
PGP**
**cheie secretă (asimetrică),
criptare, 169**
**cheie unică (simetrică), criptare,
167-168**
chmod, comandă, 123-124
chown, comandă, 123-124
-chroot director, cuvânt cheie, 227
CIAC-2319, buletin, 67
clasa A, adrese, 37
clasa B, adrese, 37
clasa C, adrese, 38
clasa D, adrese, 38
clasa E, adrese, 38
clase
adrese IP, 35-36
clasa A, 37
clasa B, 37
clasa C, 38
clasa D, 38
clasa E, 38
determinare
CH (CHAOS), 55
HS (Hesiod), 55
opțiuni, 45
clase de opțiuni, 45
Class, câmp, 55
Client Configuration, buton, 281
**clienți, configurare pentru
folosirea serverului SQUID, 256**
CNAME, tip de înregistrare, 53
**COAST (Computer Operations,
Audit and Security), sit Web, 376**

**cod de răspuns (câmpul Version
Number), 242-243**
**cod sursă, compilare (instalare
PGP sub UNIX), 190**
**cod, legare de funcțiile de
bibliotecă SOCKS, 247**
**cod, listing (exemplu de fișier
/etc/inetd.conf), 223**
coduri (ICMP), 264-265
com, domeniu organizațional, 50
**combinarea strategiilor pentru
firewall-uri, 85-88**
gazde cu două plăci de rețea,
86-87
gazde ecranate, 87-88
comentarii, inserare în fișiere, 225
comenzi
?, 233
-a politică, 260
-A regulă de înlănțuire, 268
Administrative Tools, meniu
Event Viewer, 162-163
User Manager, 158
Advanced, meniu (Proxies), 256
arp, 33
badadmin utilizator, 235
baddir director, 235
-c, 261
Category, meniu (Advanced), 256
chmod, comandă, 123-124
chown, comandă, 123-124
connect, 232
connect gazdă, 232
-d politică, 261
-D regulă de înlănțuire, 268
-D regulă de înlănțuire-regulă de
număr, 268
dbmgr, 204
directory director, 235
Edit, meniu (Network
Preferences), 256
executable program, 235
exit, 232
-F chain, 268
-f policy, 261
File, meniu
Attach to Firewall, 294
Configure New Firewall, 294
Detach From Firewall, 294
Exit, 295
Load Plan from File, 294
Print MSP Details, 295
Print MSP Summary, 295
Properties, 160-161
Retrieve Plan from Firewall, 294
Save Plan to File, 294
Save Plan to Firewall, 294
Settings, 163
finger, 155-156

Firewall, meniu
Check Alive, 296
Ping Router, 296
Restart, 296
Set Date/Time, 295
Set Password, 295
SMXP Encryption Key, 296
Upgrade, 296
gestionarea înlănțuirilor, 267
gestionarea regulilor, 268-269
groupid grup, 235-237
-h, 261
Help, 233
-i politică, 261
-I regulă de înlănțuire-regulă de
număr, 268
-l, 261
ipchains-restore, 270-271
ipchains-save, 270-271
ipfwadm, 260-263
Keys, meniu (New Key), 194
-L înlănțuire, 268
last, 155-156
Log, meniu (Security), 162-163
make, 259-260
make install, 253
maxchildren copii, 236
Microsoft Proxy Server, meniu
(Internet Service Manager), 278
-N înlănțuire, 267
-p politică, 261
-P țință de înlănțuire, 267
password, 233
PGP, 191
PGP, meniu (PGPkeys), 194
PING, 34
Policies, meniu (Audit), 158
port portid hosts, 237
Programs, meniu
Administrative Tools, 158
Microsoft Proxy Server, 278
PGP, 194
Windows NT Explorer, 160-161
Properties, meniu (Service
Properties), 277
ps, 119, 157
quit, 232
-R regulă de înlănțuire-regulă de
număr, 268
rwho, 155-156
-s top tcpfin udp, 261
sendmail program, 236
shell, 214
squid, 252-255
su, 156
timeout secunde, 233, 235-237
tn-gw proxy server, 233
Tools, meniu (Internet Options),
256
touch (UNIX), 135
TRACEROUTE, 34

UNIX
înlocuire/programe de
corectare. Vezi înlocuire
(comenzi UNIX)
programe de corectare
(comenzi UNIX), 369
userid utilizator, 235-237
View, meniu (Internet Options),
286-287
wakeupp secunde, 236
who, 155-156
-X înlănțuire, 267
x-gw, 233
-z, 261
-Z înlănțuire, 268
comenzi de nucleu, 214
comenzi PGP, 191
**Command Code, câmp (SOCKS
V5), valori, 246**
CommandView Firewall
aplicație gestionar, 293-294
descărcarea versiunii
experimentale, 287
instalare, 287-289
meniul File, 294-295
meniul Firewall, 295-296
meniul Log, 296
meniul View, 294
program de configurare, rulare,
290-293
comparare
firewall-urile FWTK și Gauntlet, 219
ipfwadm și ipchains, 264-265
**compatibilitatea protocoloalelor
IPv4 și IPv6, 310-311**
**compilarea codului sursă
(instalarea UNIX PCP), 189**
componente
FWTK, 219, 239
filozofie de proiectare, 219
instrumente de sistem, 220
instrumente software,
219-220
practici de configurare, 220
PGP Command Line, 193
PGP Eudora Plugin, 193
PGP Key Management, 193
PGP Microsoft Exchange/Outlook
Plugin, 193
PGP Microsoft Outlook Express
Plugin, 193
PGP User's Guide, 193
PGP, selectare, 192-193
PGPnet Virtual Private
Networking, 193
**componente de rețea,
monitorizare, 58**
**componente suplimentare
produse de alte firme, 280-281**
**compromiterea gazdelor bastion,
130-131**

Computer Emergency Response Team (CERT), 373-374

Computer Incident Advisory Capability, sit Web, 67

Computer Oracle and Password System (COPS), 365

comunicarea între serverele copii și părinte (SQUID), 203

comunicații în rețea, interceptare, 72-73

conectare de la distanță, 47

conectare de la distanță, 15. *Vezi* și Telnet

conectarea la baze de date, 59-60

conectări executate cu succes, auditare, 150

conexiuni

client/server, stabilire (server SOCKS), 242-244

control (PPTP), 184-185

fizice, evaluare, 34

pe linii telefonice comutate, 175

conexiuni client/server, stabilire (server SOCKS), 242-244

conexiuni de control (PPTP), 184-185

conexiuni fizice, evaluare, 34

conexiuni în rețea, control, 28-29

conexiuni pe linii telefonice comutate, 175

conexiuni protejate, asigurare, 73

configurare

modificare, 152

niveluri de severitate, 152-153

nume de utilitate, 152-153

revizuire, 154-155

transmiterea mesajelor către alte calculatoare, 154-155

asociații de securitate, 181

auditare și înregistrare în jurnal (gazde bastion), 129

avertizare prin email, 286

configurarea clienților pentru folosirea unui server SQUID, 256

filtre de pachete, 45

firewall pentru email (DNS), 236

firewall-uri, 26-27

ftp-gw, server intermediar, 229-231

gazde bastion, 112-113

informații despre serverul intermediar, 286-287

ipchains, 264

PGP (Windows NT), 194-195

plug-gw, 237

politici de auditare, 160-161

rutere cu filtrarea pachetelor, 32

servere intermediar, 227

squid, 203, 250

syslogd, 152

TCP Wrappers, 210-211

fișierul *hosts.allow*, 212-215

fișierul *hosts.deny*, 212-215

fișierul *inetd.conf*, 211-212

configurare, fișiere (syslog)

configurație bazată pe gazde ecranate, 96-97

configurații (servere SOCKS), 242-243

Configure Mail Alerting, casetă de dialog, 286

Configure New Firewall, comandă (meniul Command View File), 294

connect gazdă, comandă, 232

CONNECT, cereri, 242, 246

connect, comandă, 232

Connections, etichetă, 256

control

conexiuni de rețea, 28-29

sesiuni, 29

controllere de domeniu (Windows NT Server), 160-161

controlul accesului, 199, 208-209

controlul accesului la mediu (MAC), strat, 28-29

controlul legăturii logice (LLC), strat, 28-29

conturi (utilizatori), 250

conturi de utilizatori (squid), creare, 250

conținut (inle de chei), vizualizare, 191

conținut înglobat, 144

COPS (Computer Oracle and Password System), 365

COPS (Computer Oracle and Password System), sit Web, 365

corespondența valorilor pentru attribute, 225-226

Courtney, 367

Courtney, sit Web, 367

Crack, 364-367

Crack, sit Web, 365

creare

canale sigure, 175

conturi de utilizator (SQUID), 250

intrări secrete, 72

înălțări, 268

înălțări definite de utilizatori, 266

politici de securitate, 17-19

politici pentru firewall-uri, 18

reguli, 225-226

rețele virtuale private (VPN), 176-177

selectoare, 17

semnături digitale (PGP), 192

servere intermediar UDP, 245-246

Create Email Rule, casetă de dialog, 292-293

criptare, 167

3DES (Data Encryption Standard), 167

Blowfish, 168

cheie privată (criptare asimetrică), 169

cheie publică (criptare asimetrică), 66, 201-203, 228.

Vezi și PGP

cheie unică (simetrică), 167-168

date, 200, 217, 222. *Vezi* și IKE;

PPTP

DES (Data Encryption Standard), 168

Diffie-Hellman/DSS, 195

fișiere (PGP), 191-192, 196

fluxuri de date, 172

IDEA (International Data Encryption Algorithm), 168

PGP. *Vezi* PGP

RSA, 195

Slipjack, 168

verificarea paginilor Web, 173-174

criptare asimetrică. *Vezi* criptare

cu chei publice

criptare simetrică, 167-168

criptografie, 166

cron, program demon, 156

cutie de cristal, 220

cutie neagră, 220

cuvânt cheie, 225

cuvinte cheie, 227

accept, 266

ALL, 213

authserver gazdă port, 228

-chroot director, 227

denial-msg nume_de_fișier, 228

deny, 266

directory director, 228

-exec, program, 226

EXCEPT, 213

ftp-gw proxy, 228-229

groupid grup, 228

help-msg fișier, 228

hosts, 232

hosts gazde, 227-228

KNOWN, 213

LOCAL, 213

PARANOID, 213

plug-gw, 237

prompt prompt, 232

reject, 266

return, 266

smap, 235

smapd, 235-236

Timeout secunde, 227-229

tn-gw proxy, 232

-user userid, 227

UNKNOWN, 213

userid utilizator, 229

welcome-msg nume_de_fișier, 229

Xforwarder program, 232

D

%d, variabilă, 214

-D *adresă* [/mască] [port ...], parametru, 262

-d *destinație*, parametru, 268

-d *nivel de eroare*, parametru în linia de comandă, 253

-d *nivel de eroare*, parametru în linia de comandă, 253

-d *politică*, comandă, 261

-D *regulă de înălțuire*, comandă, 268

-D *regulă de înălțuire-regulă de număr*, comandă, 268

-D, parametru în linia de comandă, 254

DARPA (Defense Advanced Research Projects Agency), 168

Data Type, câmp, 211, 221

Datagram Length, câmp, 44

datagrame, 32, 45, 48. *Vezi* și pachete

date pentru chei, 181

dbmgr, comandă, 204

decriptare

cheie, 169

fișiere (PGP), 196

Defense Advanced Research Projects Agency (DARPA), 168

definire

rutare la sursă, 45

variabile de mediu, 189

demon, programe, 114

cron, 156

inetd, 209, 212, 221-223

mountd, 117

rpcbind, 117

sendmail, 210

syslog, 152

syslogd, 210

talkd, 116

tcpd (TCP Wrappers), 209, 211

UNIX, procese demon, 115-116

inetd.conf, fișier de configurare, 115-116

NFS (Network File System), 117

dendest-msg nume_de_fișier, cuvânt cheie, 228

denial-msg nume_de_fișier, cuvânt cheie, 228

denumirea cheilor, 190

deny, cuvânt cheie, 266

deny, politică, 261

deny, țintă, 266

deny-, modificador, 226

DES (Data Encryption Standard), 167

descărcare

CommandView Firewall (versiune de probă), 287

ipchains, 264-265

ipfwadm, 259

server SOCKS, 247-248

SOCKS V5 Reference Implementation, 247-248

SocksCap, 247

SQUID, 250

TCP Wrappers, 200

descărcarea pachetelor de servicii, sit Web, 273

Destination Address, câmp, 44, 246, 312-313

Destination IP Address, câmp

cerere BIND, 244

CONNECT Request, 242-243

Destination Port, câmp

cerere BIND, 244

CONNECT Request, 242-243, 246

Destination Unreachable, tip de mesaje, 34, 66

destinație, antet de extensie, 312-314

Detach From Firewall, comandă (meniul Command View File), 294

Details, etichetă, 173-174

detectarea intruziunilor, 306

determinarea clasei (adrese IP), 36-37

/dev/klog, dispozitiv, 152

/dev/log, soclu, 152

/drop, subdirector (directorul /rules), 205-206

dezactivarea auditării evenimentelor (Windows NT), 159

DHCP (Dynamic Host Configuration Protocol), 35, 303

diagonală la dreapta (/), 269

dial-in, posibilități, 156

dial-out, posibilități, 156

Diffie-Hellman/DSS, criptare, 195

diffuzări, 39

Digital Subscriber Line (DSL), 308

dimensiunea cheii, prompt, 190

dimensiunea cheii, specificare, 190

directoare (Windows NT), 126-127

Directory Auditing, casetă de dialog, 160-161

directory director, comandă, 235

directory director, cuvânt cheie, 228

Directory Permissions (Windows NT), casetă de dialog, 127-129

dispozitive (/dev/klog), 152

dispozitive firewall, 20, 108, 299-300

compatibilitate NAT, 303

estimarea prețului, 305

filtrarea pachetelor, 302

gestionare, 300-301

instalare, 300

interceptor, 301

interfețe de rețea, 301-302

intermediere de aplicații, 302

Lucent Managed firewall, 301-303

PERMIT, 301

plug-and-play, 301

politici de securitate, 302-303

posibilități de alarmare, 303-304

posibilități de raportare, 303-304

selectare, 305

VPN, 304

DMZ (zonă demilitarizată), 20, 85, 88-90, 220

DNS (Domain Name Service), 32

DNS (Domain Name System), 49-50</

adreselor pentru rețele private"), 38

RFC 1928, „SOCKS Protocol Version 5” („Protocolul SOCKS, versiunea 5”), 241

RFC 1929, „Username/Password Authentication for SOCKS V5” („Autentificarea prin nume de utilizator și parolă pentru SOCKS V5”), 241, 245

RFC 1961, „GSSAPI Authentication for SOCKS V5” („Autentificarea GSSAPI pentru SOCKS V5”), 241, 246

RFC 2048, „Internet Security Association and Key Management Protocol (ISAKMP)”, 180-182

RFC 2068, „HTTP status codes used in log files” („Coduri HTTP folosite în fișiere jurnal”), 255

RFC 2186, „Internet Cache Protocol (ICP) Version 2” („Protocolul ICP (Internet Cache Protocol) versiunea 2”), 203

RFC 2187, „Application of Internet Cache Protocol (ICP) Version 2” („Aplicații ale protocolului ICP (Internet Cache Protocol) versiunea 2”), 203

RFC 2412, „The Oakley Key Determination Protocol” („Protocolul Oakley de stabilire a cheii”), 181

RFC 2463, „Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)”, 311

RFC 2637, „PPTP (Point-to-Point Tunneling Protocol)”, 184

RFC 931, „Authentication Protocol” („Protocolul de autentificare”), 215

Domain Name Service (DNS), 32

Domain Name System. *Vezi* DNS

Domain Name, câmp, 54

domeniul, 49

domeniul geografice, 49

domeniul organizaționale, 49

domeniul, specificare, 268-269

Don't Fragment (DF), câmp, 44

dosare, Administrative Tools, 158

două puncte (:), 225, 269

Drawbridge, 203-205

Drawbridge Filter Compiler, 204

Drawbridge Filter Engine, 204

Drawbridge Manager, 204

Drawbridge, sit Web, 205

DSL (Digital Subscriber Line), 308

Dynamic Host Configuration Protocol (DHCP), 35, 303

E

-e, opțiune în linia de comandă, 262

-exec program, cuvânt cheie, 226

Echo Reply, tip de mesaje, 34, 65

Echo Request, tip de mesaje, 34, 65

ecranarea accesului la Internet, 144-145

Edit, meniu (Network Preferences), comandă, 256

editarea fișierelor

hosts.allow, 200

hosts.deny, 200

inetd.conf, 199

edu, domeniu organizațional, 49

educarea utilizatorilor privind

securitatea, 72

eliberarea certificatelor, 172

Elron CommandView Firewall.

Vezi CommandView Firewall

email

falsificare, 70

înșelare, 70

livrare, 283. *Vezi și* SMTP

Email Address, câmp, 54

Enable Caching, casetă de

validare, 282

Enable Dynamic Packet Filtering

on Microsoft Proxy Server

Packets, casetă de validare, 278

Enable E-Mail Notification, casetă

de validare, 292-293

Enable Logging Using, casetă de

validare, 285

Enable Packet Filtering on

External Interface, casetă de

validare, 278

Enable Web Publishing, casetă de

validare, 284

Encapsulating Security Payload

(ESP), 180, 183

ESP (Encapsulating Security

Payload), 180, 183

estimarea prețului dispozitivelor

firewall, 305

eșecuri la conectare, auditare,

150

/etc/inetd.conf, fișier, 221-222

/etc/networks, fișier (UNIX), 118

/etc/passwd, fișier, 223

/etc/protocols, fișier (UNIX), 118

/etc/services, fișier, 118, 209

/etc/syslog.conf, 182. *Vezi și*

syslog, fișier de configurare

/etc/utmp, fișier, 155-156

Ethernet 802, format de cadre, 32

etichete, 52

Alerting, 286

Certificate Path, 173-174

Connections, 256

Details, 173-174

Permissions, 281

Security, 160-161

Service, 286

evaluare

conexiuni fizice, 34

pachete IP, 266

evenimente

„I” în cerc albastru, 163

cheie, 163

lacăt, 163

semn stop, 163

semnul exclamării în cerc galben,

163

auditare (Windows NT), 158

dezactivare, 159

Event Viewer, 162-163

Print Manager, 160-161

Properties Sheet, 158

stabilirea politicilor, 160-161

User Manager, 158-161

Windows NT Explorer, 158-161

eșec la conectare, 158

File and Object Access,

eveniment, 159

Logon and Logoff, 159

Process Tracking, 159-160

Restart, Shutdown, and System,

159

Security Policy Changes, 159

succes la conectare, 158

Use of User Rights, 159

User and Group Management,

159

evenimente de eșec, înregistrare

în jurnal, 158

evenimente, pictograme, 162-163

Event Log Settings, casetă de

dialog, 163

Event Log Wrapping, buton radio,

163

Event Viewer, 157

Event Viewer, comandă (meniul

Administrative Tools), 163

EXCEPT, operator, cuvânt cheie,

213

executable program, comandă,

235

exit, comandă, 232

Exit, comandă (meniul Command

View File), 295

Expire Rate, câmp, 54

Explorer (Windows NT)

modificarea permisiunilor,

127-128

vizualizarea permisiunilor pentru

fișiere/directoare, 126-127

expresie de trecere, 189-190

expresie de trecere, prompt, 190

expresii, trecere, 189-190

F

-F chain, comandă, 268

-f policy, comandă, 261

-f, opțiune, 270-271

-F, parametru, 260, 268

-f, parametru în linia de comandă,

253-254

/facts, subdirector (directorul

/rules), 205-206

Failure, casetă de validare, 158

Farmer, Dan and Wietse Venema,

„Improving the Security of your

Site by Breaking Into It” („Cum

îmbunătățim securitatea sitului

dumneavoastră spargându-l”),

16-17, 205-206

FDDI, format de cadre, 32

Federal Computer Incidence

Response Capability, sit Web,

376

ferestre (PGP), 194

File and Object Access,

eveniment, 159

File Transfer Protocol. *Vezi* FTP

File, comenzi de meniu

Command View Firewall, 294-295

Attach to Firewall, 294

Configure New Firewall, 294

Detach From Firewall, 294

Exit, 295

Load Plan from File, 294

Print MSP Details, 295

Print MSP Summary, 295

Retrieve Plan from Firewall,

294

Save Plan to File, 294

Save Plan to Firewall, 294

Properties, 160-161

Settings, 163

filozofie de proiectare (FWTK),

219

filtrarea dinamică a pachetelor,

108, 278, 306

filtrarea pachetelor, 95-100,

258-259, 302, 306

avantaje/dezavantaje, 110-111

bitul ACK, 106

bitul SYN, 105-106

configurație pentru gazde

ecranate, 96-97

dinamică, 278, 306, 341

Drawbridge, 203-205

filtrarea dinamică a pachetelor,

108

filtrarea pachetelor independent

de stare, 82-83, 108

filtrarea pachetelor în funcție de

stare, 82-83

filtre de pachete hardware și

software, 108-109

informații de antet IP, 100-101

informații de antet TCP, 101-103

informații de antet UDP, 103-104

în funcție de stare, 306

pachete ICMP, 107

porturi, 103-105

Proxy Server, 278-280

reguli, 98-99

servicii periculoase, 99-100

socliuri, 103-104

subrețele ecranate, 97

unde să folosiți filtre de pachete,

95-98

filtrarea pachetelor independent

de stare, 82-83

filtrarea pachetelor în funcție de

stare, 82-83, 306

filtre de pachete, 13-14, 19-20, 45,

65, 81-83, 95-100

avantaje/dezavantaje, 110-111

bitul ACK, 106

bitul SYN, 105-106

combinarea cu porți intermediar

de aplicații, 85-88

gazde cu două plăci de rețea,

86-87

gazde ecranate, 87-88

configurare, 45

configurație pentru gazde

ecranate, 96-97

filtrarea dinamică a pachetelor,

108

filtrarea pachetelor independent

de stare, 82-83, 108

filtrarea pachetelor în funcție de

stare, 82-83

filtre de pachete hardware și

software, 108-109

informații de antet IP, 100-101

informații de antet TCP, 101-103

informații de antet UDP, 103-104

pachete ICMP, 107

porturi, 103-105

reguli, 98-99

convenții, 98-99

creare, 98-99

servicii periculoase, 99-100

socliuri, 103-104

subrețele ecranate, 97

unde să folosiți filtre de pachete,

95-98

filtre de pachete hardware și

software, 108-109

filtre de pachete independente de</

Forum of Incident Response and Security Teams, 372
 L0pht Heavy Industries, sit Web, 375
 liste poștale pentru firewall-uri, 375
 Microsoft, situri Web, 374
 National Security Institute's Security Resource Net, sit Web, 376-377
 SANS (System Administration, Networking and Security) Institute, 373
 securitate în NT, 375
 U.S. Department of Energy, sit Web, 376
 World Wide Web Security FAQ, sit Web, 375
 selectare, 21-22
 TCP Wrappers, 208-209
 configurare, 210-215
 controlul accesului, 208-209
 demonul tcpd, 209
 înregistrare în jurnal, 209-210
 limite, 215
 obținere, 210
 testare, 308
 translatarea adreselor, 14
 vectorizarea adreselor, 15
Firewalls, listă poștală, 375
fișier de căutare inversă, 52
fișier de configurare prestabilit (syslog), modificare, 152
fișiere
 access.log, 254
 baze de date, 52
 cache, 52
 cache.log, 254
 căutare inversă, 52
 comentarii, inserare, 225
 configurare, syslog. *Vezi* syslog,
 fișier de configurare
 configurație prestabilită (syslog),
 modificare, 152
 criptare (PGP), 191-192, 196
 criptare, acces, 192
 decriptare (PGP), 196
 /etc/inetd, fișier de configurare,
 211
 /etc/inetd.conf, 221-223
 /etc/passwd, 223
 /etc/services, 209
 /etc/utmp, 155-156
 fișier de parole ascuns (UNIX), 114
 fișiere de configurare în rețea
 (UNIX), 118
 fișiere gazdă, 139
 hosts.allow, 210
 configurare, 212-215
 editare, 200
 hosts.deny, 210
 configurare, 212-215
 editare, 200
 hosts.equiv, 56, 233
 inetd.conf, 209-210
 inetd.conf, fișier de configurare
 (UNIX), 115-116
 configurare, 211-212
 editare, 199
 keys.asc, 190-191
 lastlog, 155-156
 log, 93-94, 148-149, 164, 286
 Event, 160-161
 gestionare, 163
 revizuire, 148-151, 162-163
 specifice aplicațiilor, 164
 SQUID, 254-255
 ștergere, 150
 make, 251
 netperm-table, 272. *Vezi* și reguli
 parole, 59-60
 permisiuni, revizuire (Windows
 NT), 126-127
 -rhosts, 56, 233
 servere DNS, 52
 squid.conf, 203, 252-253
 store.log, 254
 swap.state, 255
 syslogd.conf, 210
 ștergerea fișierelor inutile de pe
 gazdele bastion, 120-121
 transferarea fișierelor între
 calculatoare, 48
 /usr/adm/wtmp, 155-156
 /var/adm/aculog, 156
 /var/log/cron, 156
fișiere ascunse de parole, 59-60,
114
fișiere criptate, acces (PGP), 192
fișiere de configurare în rețea
(UNIX), 118
fișiere de parole
 ascunse, 59-60
 sincronizare, 59-60
fișiere jurnal, 93-94, 148-149, 164,
285-286
 Application, eveniment, 161
 Event, 160-161
 gestionare (Windows NT), 163
 revizuire, 148-151, 162-163
 Security, eveniment, 162-163
 specifice aplicațiilor, 164
 SQUID, 254-255
 System, eveniment, 161
 ștergere, 150
 UNIX, 155-156
fișiere jurnal pentru evenimente,
160-161
fișiere jurnal specifice aplicațiilor,
164
fizic, strat, 28

Flags, câmp, 44
Flow Label, câmp, 312
flux de date, 101
flux de date, criptare, 172
foaie de proprietăți, 158, 161
formate de cadre, 32
Forum of Incident Response and
Security Teams, sit Web, 372
Forward, înălțuire pentru
retransmitere, 265
FQDN (nume de domenii
complete), 50
Fragment Offset, câmp, 44, 68
fragmentare (UDP), 246
fragmentare, antet de extensie,
312-314
fragmentarea pachetelor, 68-69,
246
frecvență, schimbarea cheilor,
181
Free Software Foundation, 249
Free Software Foundation, sit
Web, 249
FreeBSD, 204
FreeBSD, sit Web, 204
freeware, 198
FTP (File Transfer Protocol), 18,
26-27, 48, 208
 dezavantaje, 48
 programe de corectare (SRA),
 370
ftp-gw, 228
ftp-gw proxy, 228
 configurare, 229-231
 cuvinte cheie, 228-229
funcții de bibliotecă (SOCKS),
legarea codului, 247
funcții de rețea (WinSock),
interceptarea apelurilor, 241,
247
FWTK (Firewall Toolkit), 84,
200-201, 217-218, 259
 authd, 201
 comparat cu firewall-ul Gauntlet,
 219
 componente, 219-220, 239
 ftp-gw, 201
 instalare (gazde bastion),
 239-240
 istoric, 217-218
 login-sh, 201
 netact, 201
 obținere, 218
 plug-gw, 201
 rlogin-gw, 201
 smap, 201
 smapd, 201
 syslogd, 201
 telnetd, 201
 tn-gw, 201
FWTK, sit Web, 217-218, 240

G

Gabriel, 367
Gabriel, sit Web, 367
Gauntlet, firewall, 200, 219
gazdă de încredere, 73-74
gazde
 bastion, 20, 89-92, 112-113
 auditare și înregistrare în jurnal,
 configurare, 129
 compromiterea gazdelor
 bastion, 130-131
 configurare, 112-113
 instalarea setului FWTK,
 239-240
 servicii Windows NT, 119-120
 sisteme de operare sigure,
 instalare pornind de la zero, 114
 software intermediar, rulare,
 129-130
 ștergerea aplicațiilor și
 fișierelor inutile, 120-121
 UNIX, fișiere de configurare
 pentru rețea, 118
 UNIX, permisiuni pentru
 resurse, 121-124
 UNIX, procese demon, 115-116
 Windows NT, permisiuni pentru
 resurse, 125-129
 cărora li se acordă încredere, 73-74
 de sacrificiu, 20
 gazde cu două plăci de rețea,
 86-87, 109
 gazde de sacrificiu, 89-92
 gazde ecranate, 87-88
 reconfigurare (atacuri prin
 blocarea unui serviciu), 63
gazde bastion, 20, 85, 89-92,
112-113
 auditare și înregistrare în jurnal,
 configurare, 129
 compromiterea gazdelor bastion,
 130-131
 configurare, 112-113
 eliminarea aplicațiilor și fișierelor
 inutile, 120-121
 instalarea setului FWTK, 239-240
 servicii Windows NT, 119-120
 sisteme de operare sigure,
 instalare pornind de la zero, 114
 software intermediar, rulare,
 129-130
 UNIX, fișiere de configurare
 pentru rețea, 118
 UNIX, permisiuni pentru resurse,
 121-124
 SGID (Set Group ID), 122-123
 SUID (Set User ID), 122-123
 valori pentru permisiuni,
 modificare, 123-124
 valori pentru permisiuni,
 vizualizare, 122
 valori pentru proprietar,
 modificare, 123-124
 UNIX, procese demon, 115-116
 Windows NT, permisiuni pentru
 resurse, 125-129
 modificare, 127-129
 permisiuni speciale, 125
 permisiuni standard, 125-126
 vizualizare pentru
 fișiere/directoare, 126-127
gazde cu două plăci de rețea,
86-87, 109
gazde de sacrificiu, 20, 89-92
gazde ecranate, 87-88
găsirea buletinelor informative, 67
generarea perechilor de chei
publică/secretă
 instalarea PGP sub UNIX,
 189-190
 instalarea PGP sub Windows NT,
 194-195
generarea perechilor de chei
publice/private
 instalare UNIX PGP, 189-190
 instalare Windows NT PGP,
 194-195
gestionare
 dispozitive firewall, 300-301
 fișiere jurnal (Windows NT), 163
 înălțuirii, 267
 proprietăți pentru păstrarea în
 cache, 282-284
 reguli, 268-269
 servicii pentru utilizatori, 297
 SQUID, 252
GIAC (Global Incident Analysis
Center), 373
GNU, 249
gov, domeniu organizațional, 50
groupid grup, comandă, 235-237
groupid grup, cuvânt cheie, 228
GSS-API, autentificare, 246

H

-h, comandă, 261
-h, parametru în linia de comandă,
253
%h, variabilă, 214
hackeri, 70
Header Checksum, câmp, 44
Help, comandă, 233
help-msg fișier, cuvânt cheie, 228
HIINFO, tip de înregistrare, 53
Hop Limit, câmp, 312
hosts gazde, cuvânt cheie, 227-228
hosts, atribut, opțiune, 229, 232
 valori pentru permisiuni,
 modificare, 123-124
 valori pentru permisiuni,
 vizualizare, 122
 valori pentru proprietar,
 modificare, 123-124
 UNIX, procese demon, 115-116
 Windows NT, permisiuni pentru
 resurse, 125-129
 modificare, 127-129
 permisiuni speciale, 125
 permisiuni standard, 125-126
 vizualizare pentru
 fișiere/directoare, 126-127
hosts, cuvânt cheie, 232
hosts, fișiere, 139
hosts.allow, fișier, 210
 configurare, 212-215
 editare, 200
hosts.deny, fișier, 210
 configurare, 212-215
 editare, 200
hosts.equiv, fișier, 56, 233
Hosttype, subdirector (directorul
/rules), 205-206
HS (Hesiod), clasă, 55

-i interfață, parametru, 268
-i politică, comandă, 261
-l regulă de înălțuire-regulă de
număr, comandă, 268
-l, parametru, 260
„I” în cerc albastru, 163
IANA (Internet Assigned Numbers
Authority), 46, 245, 317
ICMP (Internet Control Messages
Protocol), protocol, 33-35, 311
 coduri, 98, 264-265
 mesaje pentru oprirea sursei, 107
 pachete, 34, 107
 tipuri, 264-265
 tipuri de mesaje, 34, 65-66
ICP (Internet Cache Protocol),
203, 255
IDEA (International Data
Encryption Algorithm), 168
IDENT, protocol, 245
Identification, câmp, 44
ierarhie (DNS), 50
ierarhie de cache (SQUID), 255
ieșire numerică, 270
ieșiri numerice, 270
IETF (Internet Engineering Task
Force), 184
IETF, sit Web, 173-174
ifstatus, 367
ifstatus, sit Web, 367
IKE (Internet Key Exchange),
180-182
IKE SA, 181
imprimante
 auditarea utilizării, 161
 foi de proprietăți, 158
„Improving the Security of your
Site by Breaking Into It” (Dan
Farmer & Wietse Venema), sit
Web, 16-17, 205-206
IN, câmp, 53-55
indicatoare
 bidirecționale, 270
 înregistrare în jurnal, 270
 More Fragments (MF), 44
 pentru mai multe informații, 270

indicator bidirecțional, 269
 indicator pentru înregistrare în
 jurnal, 270
 inele de chei, 190-191
 inetd, 199
 inetd, program demon, 209, 212,
 221-223
 inetd, server demon, 116
 inetd.conf, fișier, 209-210
 inetd.conf, fișier de configurare
 (UNIX), 115-116
 configurare, 211-212
 editare, 199
 Information Reply, tip de mesaje,
 34-35
 Information Request, tip de
 mesaje, 34-35
 informații de antet TCP (filtre de
 pachete), 101-103
 informații DNS (servere
 intermediare clasice), 138-139
 informații în rețea, reconfigurare
 (atacuri prin blocarea unui
 serviciu), 63
 informații pentru serverul
 intermediar, configurare,
 286-287
 Input, înlănțuire de intrare, 265
 inserarea comentariilor în fișiere,
 225
 inspectare în funcție de stare, 108
 instalare
 dispozitive firewall, 300
 Drawbridge, 204
 firewall-uri (CommandView
 Firewall), 287-289
 FWTK, gazdă bastion, 239-240
 ipchains, 264
 ipfwadm, 259-260
 Microsoft Proxy Server, 273-277
 pachete de servicii, 273
 partiții NTFS, 274
 program de instalare, 274
 PGP, 189
 UNIX, 189-190
 Windows NT, 192-193
 sisteme de operare sigure,
 instalare pornind de la zero, 114
 SQUID, 250-252
 Installation Options (Microsoft
 Proxy Server, configurare),
 casetă de dialog, 274
 instrucțiuni de utilizare
 acceptabilă (politici de
 securitate), 77-78
 instrumente
 auditare IP (Argus), 366
 monitorizarea rețelei, 366
 Argus, 366
 Courtney, 367
 Gabriel, 367

ifstatus, 367
 ISS (Internet Security
 Scanner), 366
 Merlin, 368
 NID (Network Intrusion
 Detector), 368
 SATAN (Security Administrator
 Tool for Analyzing Networks),
 366-367
 SWATCH (Simple WATCHer),
 366
 tcpdump, 368
 verificarea securității sistemului,
 368
 Isof (List Open Files), 369
 MD5, 369
 Secure Sun, 368
 Tripwire, 369
 trojan.pl, 368
 Instrumente de sistem (FWTK),
 220
 Instrumente pentru monitorizarea
 rețelei. *Vezi* instrumente,
 monitorizarea rețelei
 Instrumente pentru verificarea
 securității sistemului, 368-369
 instrumente software (FWTK),
 219-220
 int, domeniu organizațional, 50
 integrarea firewall-urilor, 307
 integritatea datelor, 166, 170-171
 interceptare
 apeluri (funcții de rețea WinSock),
 241, 247
 comunicații în rețea, 72-73
 pachete, 73
 Interceptor, dispozitiv firewall,
 301
 interfete (rețea), dispozitive
 firewall, 301-302
 interfețe de rețea
 dispozitive firewall, 301-302
 în modul eterogen, localizare, 367
 Interfețe în mod de lucru
 eterogen, localizare, 367
 intermediar de aplicații, 13-14,
 19-20, 84, 303
 intermediar, aplicații
 aplicații, 13-14, 19-20, 84, 302
 ftp-gw, 228
 configurare, 229-231
 cuvinte cheie, 228-229
 intermediar clasic, 135-139
 intermediar de aplicații, 84
 intermediare proprii, creare, 139
 intermediare transparente,
 137-138
 Remote Login, 233
 rlogin, 233
 Telnet, 231

tn-gw, 231-232
 UDP, creare, 245-246
 intermediare clasice, 135-139
 intermedierea aplicațiilor, 306
 International Data Encryption
 Algorithm (IDEA), 168
 International Standardization
 Organization (ISO), 26-27
 Internet, 306
 acces
 blocaje, 144-145
 ecranare, 144-145
 restricționare, 15
 politici de securitate, creare,
 17-19
 securitate, 16-17
 utilizări, 17-18
 Internet Assigned Numbers
 Authority (IANA), 46, 245, 317
 Internet Cache Protocol (ICP),
 203, 255
 Internet Control Message
 Protocol. *Vezi* ICMP
 Internet Daemon, 243. *Vezi și*
inetd
 Internet Engineering Task Force
 (IETF), 184
 Internet Header Length (IHL),
 câmp, 43
 Internet Key Exchange (IKE),
 180-182
 Internet Options, casetă de
 dialog, 256
 Internet Options, comandă
 meniul Tools, 256
 meniul View, 286-287
 Internet Protocol. *Vezi* IP
 Internet Security Association and
 Key Management Protocol
 (ISAKMP), 180-182
 Internet Security Scanner (ISS),
 366
 Internet Service Manager, 277
 Internet Service Manager,
 comandă (meniul Microsoft
 Proxy Server), 278
 Internet, serviciu (Proxy Server),
 286-287
 întimitate, 166
 intrare
 în matrice de servere intermediar,
 280-281
 în rețele virtuale private, 176
 Intrări secrete, creare, 72
 investigații sociale, 24
 IP (Internet Protocol), 31-32, 62,
 73-74, 208, 309-310
 IP, adrese, 33-35
 Remote Login, 233
 rlogin, 233
 Telnet, 231
 alocare, 303
 lungime, 35
 notația zecimală cu punct, 35-36

specificare, 268-269
 translatate, 32
 IP, anteturi, 43-45
 IP, câmpuri în antet, protecție,
 182-183
 IP, clase de adrese, 35-36
 clasa A, 37
 clasa B, 37
 clasa C, 38
 clasa D, 38
 clasa E, 38
 determinare
 IP, informații de antet, 100-101
 IP, instrumente de auditare, 366
 IP, înșelare, 44, 98
 IP, pachete, 43, 73, 266
 IP, reguli de contorizare a
 pachetelor, 259-260
 IP, reguli de ieșire pentru firewall,
 259-260
 IP, reguli de intrare în firewall,
 259-260
 IP, reguli de retransmitere în
 firewall, 259-260
 IP, retransmitere, 86, 134
 IP, strat, 43
 Ipchains, 258-259, 271
 Ipchains, sit Web, 264-265,
 270-271
 Ipchains-restore, comandă,
 270-271
 Ipchains-save, comandă, 270-271
 comparație cu ipfwadm, 264-265
 configurare, 264
 descărcare, 264-265
 instalare, 264
 înălțurii, 265-267
 opțiuni în linia de comandă, 269
 ipfw, 259
 ipfwadm, 258-259, 270-271
 ipfwadm, comandă, 260-263
 ipfwadm, reguli, 264
 comenzi, 260-261
 comparație cu ipchains, 264-265
 descărcare, 259
 instalare, 259-260
 parametri, 262
 reguli, 259-260
 sit Web, 259
 IPSec, suită de protocoale,
 179-180
 IPv4, 179, 309-310
 IPv6, 179, 309-310, 314-315
 IPv6 Forum, sit Web, 309-310
 IPv6, adresare (compatibilitate),
 245
 IPv6, sit Web, 309-310
 adrese, 314
 anteturi cu lungime fixă, 309-312
 anteturi de extensie, 312-314
 compatibilitate cu IPv4, 310-311

ISAKMP (Internet Security
 Association and Key
 Management Protocol), 180-182
 ISO (International Standardization
 Organization), 26-27
 ISS (Internet Security Scanner), 366
 ISS, situri Web, 366
 istoricul firewall-ului FWTK, 217-218

I

îmbunătățirea performanțelor, 15
 împărțirea adreselor (măști de
 subrețea), 41
 împărțirea în subrețele, 41
 încapsulare, 32
 încapsularea conținutului de
 securitate, antet de extensie,
 312-313
 înălțuire de ieșire (Output), 265
 înălțurii definite de utilizatori,
 266-267
 înălțurii, 323-326. *Vezi și* reguli
 creare, 268
 definite de utilizator, 266-267
 gestionare, 268
 ieșire, 265
 intrare, 265
 retransmitere, 265
 înlocuitor pentru programul de
 mapare a porturilor (PortMap
 V3), 370
 înlocuitori (comenzi UNIX),
 369-370
 înlocuitori pentru programul
 finger, 370
 înregistrare în jurnal, 209-210,
 285-286
 evenimente, 158
 gazde bastion, configurare, 128
 Regular, format, 285
 servere intermediar, 145
 TCP Wrapper (demonul syslogd),
 200
 Verbose, format, 285
 înregistrare în jurnal la distanță,
 47
 înregistrări, 152
 acțiuni, 152-153
 resurse, 52-53
 selectoare, 152-153
 SOA (Start of Authority), 52-54
 înregistrări de resurse, 51-53
 înregistrări de resurse DNS, 52-53
 înșelare
 adrese IP, 98
 email, 70, 73-74
 întărirea calculatoarelor pentru
 gazde bastion, 112-113
 fișiere de configurare în rețea,
 UNIX, 118

proces demon UNIX, 115-116
 servicii Windows NT, 119-120
 sisteme de operare sigure,
 instalare pornind de la zero, 114
 întreruperea alimentării, 24
 întreruperi fizice, 24
 întreținerea firewall-urilor, 24-25

J

-j *fișier*, parametru, 268
 Join Array, casetă de dialog,
 280-281

K

-k check, parametru în linia de
 comandă, 253
 -k debug, parametru în linia de
 comandă, 253
 -k interrupt, parametru în linia de
 comandă, 253
 -k kill, parametru în linia de
 comandă, 253
 -k rotate, parametru în linia de
 comandă, 253
 -k shutdown, parametru în linia de
 comandă, 253
 -k, opțiune în linia de comandă,
 262
 -k, parametru în linia de comandă,
 253
 Kerberos, 60
 Key Generation Wizard, 194, 196
 Key Generation Wizard, casetă de
 dialog, 194
 key user ID, prompt, 190
 Keys, meniu (New Key), 194
 keys.asc, fișier, 190-191
 KNOWN, cuvânt cheie, 213
 Koblas, David, 241

L

-L *înălțuire*, comandă, 268
 -l, comandă, 261
 -l, opțiune în linia de comandă,
 270
 L0pht Heavy Industries, sit Web,
 375
 L2TP (Layer Two Tunneling
 Protocol), 186
 Iacăt, pictogramă, 163
 LAN Settings, buton, 256
 LANS (rețele locale), 58
 informații despre LAN, ascundere
 prin NAT, 142
 securitate, 58
 autentificarea utilizatorilor, 59-60
 măsurile de protecție fizice, 61
 protejarea resurselor, 60-61

spațiu de adrese, creștere cu NAT, 142-143

lansare

- plug-gw, 237
- smap, 236
- syslog, demon, 152

last, comandă, 155-156

lastlog, fișier, 155-156

Layer Two Tunneling Protocol (L2TP), 186

Lee, Ying-Da, 241

legarea codului de funcțiile de bibliotecă SOCKS, 247

legătură de date, strat OSI, 28-29

legături sigure, 378. Vezi și VPN

Length, câmp, 183

Lightweight Internet Cache Protocol (ICP), 203, 255

linii închiriate, 175

liniută de despărțire (-), 226

Linux, 151

List Open Files (lsdf), 369

liste pentru controlul accesului (rutere), 108-109

liste poștale

- firewall-uri, 375
- SOCKS, 247-248
- Tiger, 366

livrarea mesajelor email, 15, 283. Vezi și SMTP

Load Plan from File, comandă (meniul Command View File), 294

Local Address Table, buton, 281

Local Area Network (LAN)

- Settings, casetă de dialog, 146-147, 256

LOCAL, cuvânt cheie, 213

localizarea interfețelor de rețea care lucrează în modul eterogen, 367

Log to File, buton radio, 285

Log to SQL/ODBC, buton radio, 285

Log, comenzi de meniu (Security), 163

Log, meniu (firewall-ul CommandView), 296

Login and Logout, eveniment, 159

login-sh, 201, 220

lsdf (List Open Files), 369

lsdf, sit Web, 369

Lucent Managed Firewall, dispozitiv firewall, 301-303

lungimea adreselor IP, 35

M

-m markvalue, opțiune în linia de comandă, 270

-m, opțiune în linia de comandă, 262

-M, parametru, 260

MAC, adrese, 32-35

make install, comandă, 253

make, fișier, 259-260

man, pagini, 226

manipularea cererilor de la clienți, 284

Manual Proxy Configuration, buton radio, 256

masq, țintă, 266

master secret, 172

Master Security Plan, 294-295

matrice (servere intermediar), intrare în, 280-281

matrice de permisiuni, 122

maxchildren copii, comandă, 236

Maximum Log Size, câmp, 163

măști de rețea, specificare, 268

măști de subrețea, 40-42

măști de subrețea cu logică booleană, 40

MB, tip de înregistrare, 54

MD5, 369

Merlin, 367

Merlin, sit Web, 367

mesaj de oprire a sursei, 34

mesaje

- date, 101
- transmiterea către alte calculatoare (fișier de configurare pentru syslog), 154-155

metodă de conectare prin confirmare în trei etape, 64

metode de autentificare (SOCKS V5), 245

metode de conectare, dialog pe trei direcții, 64

metode de difuzare (ARP), 33

MG, tip de înregistrare, 54

Microsoft Point-to-Point Tunneling Protocol. Vezi PPTP

Microsoft Proxy Server, comandă (meniul Programs), 278

Microsoft Proxy Server, meniu (Internet Service Manager), 278

Microsoft Proxy Server. Vezi Proxy Server

Microsoft, situri Web, 114, 374

descărcarea pachetelor de servicii, 273

securitate, 374

mil, domeniu organizațional, 50

MINFO, tip de înregistrare, 53

Minimum TTL, câmp, 54

mod de lucru principal, 181

mod rapid, 181

modele de rețea (OSI), 27-28

modele, straturi, 28

modemuri pentru cablu, 308

modificarea fișierului prestabilit de configurare (syslog), 152

modificatori

- deny-, 226
- permit-, 226

modul agresiv, 181

modul de transport, 183

modul tunel, 183

moduri

- agresiv, 181
- principal, 181
- rapid, 181
- transport, 183
- tunel, 183

monitorizare

- componente de rețea, 58
- rețea (instrumente), 366
- Argus, 366
- Courtney, 367
- Gabriel, 367
- ifstatus, 367
- ISS (Internet Security Scanner), 366
- Merlin, 367
- NID (Network Intrusion Detector), 368
- SATAN (Security Administrator Tool for Analyzing Networks), 366-367
- SWATCH (Simple WATCHer), 366
- tcpdump, 368
- trafic de rețea, 72-73

More Fragments (MF), indicator, 44

motoare de căutare (altavista), 372

mountd, program demon, 117

MR, tip de înregistrare, 54

MX, tip de înregistrare, 54

N

%n, variabilă, 214

-N înlănțuire, comandă, 267

-n, opțiune în linia de comandă, 262, 270

-N, parametru în linia de comandă, 254

Name, câmp, 211, 221

NAPT (Network Address Port Translation), 141-142

NAT (Network Address Translation), 139-144, 303

- alocarea dinamică a adreselor, 140
- comparație cu vectorizarea adreselor, 143
- NAPT (Network Address Port Translation), 141-142
- NAT de bază, 140-141
- rețele locale (LAN), 142-143

NAT (Network Address Translation), funcționalitate, 300

NAT (translatarea adreselor de rețea), 23

NAT de bază (translatarea adreselor de rețea), 140-141

National Security Institute's Security Resource Net, sit Web, 376-377

NDS (Novell Directory Services), 60

nerepudiare, 171

net, domeniu organizațional, 50

netaci, 201, 221-225, 227

netaci, aplicație, 223

NetBIOS (Windows NT), protocol, 119-120

netdemon, repornire, 211

netperm-table, fișier, 272. Vezi și reguli

Network Address Port Translation (NAPT), 141-142

Network Address Translation (NAT), funcționalitate, 300

Network Address Translation. Vezi NAT

Network Associates, sit Web, 188

Network File System (NFS), 99, 117

Network Information Center (NIC), 44

Network Information Service (NIS), 59-60, 100

Network Intrusion Detector (NID), 368

Network News Transport Protocol (NNTP), 236

Network Preferences, comandă (meniul Edit), 256

Network, miniaplicație (Windows NT)

New Key, comandă (meniul Keys), 194

Next Header, câmp, 312

NFS (Network File System), protocol, 117

NIC (Network Interface Center), 44

NID (Network Intrusion Detector), 368

NID, sit Web, 368

NIS (Network Information Service), 59-60, 100

niveluri de severitate (fișier de configurare syslog), 152-153

NNTP (Network News Transport Protocol), 236

noduri (conexiuni de rețea), control, 28-29

notația zecimală cu punct, 35-36

Novell Directory Services (NDS), 60

NS, tip de înregistrare, 53-54

NT, securitate, sit Web, 375

NTFS, partiții, 274

NULL, tip de înregistrare, 54

nume complete de domenii (FQDN), 50

nume de conturi, 58

nume de domenii (acceptare), 245

nume de gazde, 33

nume de utilitare/fișier de configurare syslog), 152-153

nume de utilizatori, 58

numere de opțiuni, 45

numere de porturi, 46, 222, 268-269, 317

numere de porturi recunoscute (TCP/UDP), 318-363

O

-o [maxsize], opțiune în linia de comandă, 270

-o, opțiune în linia de comandă, 262

-O, parametru, 260

Oakley, metodă de schimbare a cheilor, 180

obținere

- FWTK, 218
- TCP Wrappers, 210

octeți, 44

Open System Interconnect (OSI), 26-27

operator, cuvinte cheie (EXCEPT), 213

Options, câmp, 45

opțiuni

- auth, 232
- f, 270-271
- passok, 232
- plug-to gazdă, 238
- port portid, 238
- privport, 238
- v, 270-271
- hosts, atribut, 229, 232
- plug-gw, 238

opțiuni în linia de comandă

- b, 262, 263
- e, 262
- k, 262
- l, 270
- m, 262
- m markvalue, 270
- n, 262, 270
- o, 262
- o [maxsize], 270
- r port, 262
- t andmask ormask, 270
- t andmask xormask, 263
- v, 263, 270
- x, 263, 270

-x, 263, 270

ipchains, 269

ipfwadm, comandă, 262-263

org, domeniu organizațional, 50

OSI (Open System Interconnect), 26-27

OSI, model de rețea, 27-28

P

%p, variabilă, 214

-p politică, comandă, 261

-P protocol, parametru, 262, 268

-P țintă de înlănțuire, comandă, 267

-passok, opțiune, 232

-plug-to gazdă, opțiune, 238

-port portid, opțiune, 238

-privport, opțiune, 238

pachete de răspuns, 246

pachete de servicii, 273

pachete pentru cereri (UDP ASSOCIATE), 246

pachete, 69. Vezi și datagrame

- cerere (UDP ASSOCIATE), 246
- filtrare, 258-259, 302
- dinamică, 306
- Drawbridge, 203-205
- în funcție de stare, 306
- fragmentare, 246
- ICMP, 34
- interceptare, 73
- IP, 73
- pachete ICMP, 107
- răspuns, 246
- transferare, 31-32

Padding, câmp, 45

pagini de manual, 226

pagini de proprietăți

- Caching, 282-283
- Logging, 284
- Permissions, 281-282
- Publishing, 284-285
- Routing, 284
- Service, 281

pagini Web, verificarea criptării, 173-174

Parameter Problem, tip de mesaje, 34

parametri

- A direcție, 260
- D adresă [mask] [port ...], 262
- d destinație, 268
- F, 260, 268
- l, 260
- i interfață, 268
- j țintă, 268
- M, 260
- O, 260
- P protocol, 262, 268

-S adresă [/mask] [port ...], 262
 -s sursă, 268
 -V adresă, 262
 -W nume, 262
 ipfwadm, 262
 în linia de comandă (comanda squid), 253-254
 reguli, specificare, 268
parametri în linia de comandă (comanda squid), 253-254

-a port, 253
 -D, 254
 -d nivel de eroare, 253
 -f, 253-254
 -h, 253
 -k, 253
 -k check, 253
 -k debug, 253
 -k interrupt, 253
 -k kill, 253
 -k rotate, 253
 -k shutdown, 253
 -N, 254
 -R, 254
 -s, 254
 -u, 254
 -V, 254
 -X, 254
 -Y, 254
 -y, 254

PARANOID, cuvânt cheie, 213

parole, 59-60, 71

parole, utilitare

COPS (Computer Oracle and Password System), 365
 Crack, 364-367
 Perl COPS (Computer Oracle and Password System), 365
 Tiger, 365

partiții FAT, transformarea în partiții NTFS, 274

partiții, FAT/NTFS, 274

password, comandă, 233

Payload Length, câmp, 312

paznicii porții, 95

părinte, procese de fundal, 252

părinte, servere, 203

părinte, servere de cache, 255

păstrare în cache, 14

pătrunderi în sistem, 71, 149

PCERT (Purdue Computer Emergency Response Team), sit Web, 373-374

performanțe, îmbunătățire, 15

Perl COPS (Computer Oracle and Password System), 365

Perl COPS (Computer Oracle and Password System), sit Web, 365

permisiuni. Vezi permisiuni pentru resurse

permisiuni pentru resurse

UNIX

SGID (Set Group ID), 122-123
SUID (Set User ID), 122-123
valori pentru permisiuni, modificare, 123-124
valori pentru permisiuni, vizualizare, 122
valori pentru proprietar, modificare, 123-124
 vizualizare pentru
 fișiere/directoare, 126-127
 Windows NT, 125-129
modificare, 127-129
permisiuni speciale, 125
permisiuni standard, 125-126

permisiuni speciale (Windows NT), 125

permisiuni standard (Windows NT), 125-126

Permission, etichetă, 281

Permissions, pagină de proprietăți, 281-282

PERMIT, dispozitiv firewall, 301

permit-, modificador, 226

PGP (Pretty Good Privacy), software de criptare, 169, 175, 188, 191-192

configurare (Windows NT), 194-195

criptarea fișierelor, 196

decriptarea fișierelor, 196

fișiere criptate, acces, 192

instalare, 190

UNIX, 189-190

Windows NT, 192-193

selectarea componentelor, 192-193

semnături digitale, creare, 192

PGP Command Line, componentă, 193

PGP Eudora Plugin, componentă, 193

PGP Key Management, componentă, 193

PGP Microsoft Exchange/Outlook Plugin, componentă, 193

PGP Microsoft Outlook Express Plugin, componentă, 193

PGP User's Guide, componentă, 193

PGP, comandă (meniul Programs), 194

PGP, comenzi de meniu (PGPkeys), 194

PGP, fereastră, 194

PGPkeys, comandă (meniul PGP), 194

PGPnet Virtual Private

Networking, componentă, 193

pictogramă cu semnul stop, 163

pictogramă pentru chei, 163

pictograme pentru evenimente, 162-163

„I” în cerc albastru, 163

cheie, 163

lăcăț, 163

semn stop, 163

semnul exclamării în cerc galben, 163

PING, 65-66, 311

PING of Death, prevenire, 66

Ping Router, comandă (meniul CommandView Firewall), 296

PING, comandă, 34

plăci adaptoare (rețea), revizuire, 290

plăci de rețea, revizuire, 290

plug-and-play, dispozitive firewall, 301

plug-gw, 220, 236-238

plug-gw, poartă, 139

configurare, 237

cuvinte cheie, 237

lansare, 237

opțiuni, 238

Plugs, buton, 280-281

poartă intermediar de aplicații, 83-88

Point-to-Point Protocol (PPP), protocol, 184, 303

Point-to-Point Tunneling Protocol. Vezi PPTP

Policies, comenzi de meniu (Audit), 158

politici

firewall-uri, creare, 18

interzicere, 261

respingere, 261

securitate, 16-19

politici de auditare, configurare, 160-161

politici de conectare în rețea (politici de securitate), 76-77

politici de securitate, 16, 75-79

creare, 17-19

discutarea elementelor specifice cu angajații, 78-79

instrucțiuni de utilizare acceptabilă, 77-78

politica de conectare la rețea, 76-77

raportarea incidentelor și răspunsul la acestea, 92-93

politici pentru firewall-uri, 79-81

port portid hosts, comandă, 237

port TCP, 46

Port, câmp, 256

PortMap V3, 370

PortMap V3, sit Web, 370

porturi înregistrate, 47, 317

porturi privilegiate, 104

porturi recunoscute, 46-47, 317

porturi, 396-397. Vezi și

protocoale

domeniu, 268-269

filtre de pachete, 103-105

înregistrate, 47, 245

porturi privilegiate, 104

recunoscute, 46-47, 317

TCP, 46

UDP, 46

porți

aplicații, 264, 296- Vezi și

intermediar de aplicații; server

intermediar

intermediar (rlogin-gw), 233-234

la nivel de circuit, 245

porți de aplicații, 83, 132-135, 245

avantaje și dezavantaje, 135

blocarea traficului IP, 135

dezactivarea rutării, 134

server intermediar, 217-218

porți intermediar (rlogin-gw), 233-234

porți la nivel de aplicație, 140

porți la nivel de circuit, 140, 245

posibilități de avertizare (dispozitive firewall), 303-304

posibilități de raportare (dispozitive firewall), 303-304

PPP (Point-to-Point Protocol), protocol, 184, 303

PPTP (Point-to-Point Tunneling Protocol), protocol, 176-177, 184

PPTP, conexiuni de control, 184-185

PPTP, tuneluri, 184-185

practici de configurare (FWTK), 220

premaster secret, 172

Pretty Good Privacy, software de criptare. Vezi PGP, software de

criptare

prevenire

atacuri prin blocarea unui

serviciu, 63

inundare SYN, 64-65

Ping of Death, 66

prezentare, strat OSI, 27, 30

Primary Server, câmp, 54

Print Manager, 160-161

Print MSP Details, comandă (meniul Command View File), 295

Print MSP Summary, comandă (meniul Command View File), 295

proceduri de raportare și răspuns la incidente (politici de securitate), 92-93

proces copii, 252

Process arguments, câmp, 211, 222

Process Tracking, eveniment, 159-160

program de instalare (CommandView Firewall), rulare, 290-293

programe de corectare (comenzi UNIX), 369

Authentication Server Daemon (Authd), 370

instrumente r (ssh), 371*

sendmail (smrsh), 369

su (program fals), 371

Telnet/FTP (SRA), 370

programe pentru controlul accesului, 267. Vezi netacl

Programs, comenzi de meniu

Administrative Tools, 158

Microsoft Proxy Server, 278

PGP, 194

Windows NT Explorer, 160-161

proiectarea firewall-urilor, 75-81

politici de securitate, 75-79

discutarea elementelor

specifice cu angajații, 78-79

instrucțiuni de utilizare acceptabilă, 77-78

politica de conectare la rețea, 76-77

raportarea incidentelor și

răspunsul la acestea, 92-93

politici pentru firewall-uri, 79-81

strategii, 81-87, 89-92

arhitectură de subrețea

ecranată, 88-90

combinarea strategiilor, 85-88

filtre de pachete, 81-83

gazde bastion, 89-92

gazde de sacrificiu, 89-92

porți pentru intermedierea

aplicațiilor, 83-84

prompt prompt, cuvânt cheie, 232

prompturi, 189-190

Properties, comandă (meniul File), 160-161

Properties, comenzi de meniu (Service Properties), 277

proprietăți păt cache, gestionare, 282-284

protejare, 182-183

câmpuri în antetul IP, 182-183

parole, 71

protejarea resurselor, 60-61, 151

protocoale de dialog, SSL (Secure Sockets Layer), 172-173

protocoale de înregistrare, SSL (Secure Sockets Layer), 172

protocoale de rețea

probleme de securitate, 61-62

TCP/IP, 208

protocoale. Vezi și porturi

ARP (Address Resolution Protocol), 26-27, 32-33

bootp, 35

de rețea (TCP/IP), 208

FTP, 26-27, 48

ICMP (Internet Control Messages Protocol), 33-35

IDENT, 245

IP (Internet Protocol), 31-32, 62,

309-310

înregistrare (SSL), 172

NetBIOS (Windows NT), 119-120

NFS (Network File System), 117

PPP (Point-to-Point Protocol), 184, 303

PPTP (Point-to-Point Tunneling Protocol), 176-177, 184

protocol de dialog (SSL), 172-173

SMTP (Simple Mail Transfer Protocol), 55

SOCKS, 241

SSL (Secure Sockets Layer), 169, 172-173, 175

TCP (Transmission Control Protocol), 32, 64

TCP/IP. Vezi TCP/IP

TFTP, 49

TLS (Transfer Layer Security), 173-174

UDP, 26-27, 32

Protocol, câmp, 211, 221

Proxies, comandă (meniul Advanced), 256

Proxy Address to Use, câmp, 256

Proxy Server, 96-97, 158, 160-161,

247, 264, 296, 334-335. Vezi și

intermediar de aplicații, poartă de aplicații

intrarea în matrice de servere intermediar, 280-281
 înregistrare în jurnal, 145
 Logging, pagină de proprietăți, 284
 păstrare în cache, 249
 Permission, pagină de proprietăți, 281-282
 Publishing, pagină de proprietăți, 284-285
 Routing, pagină de proprietăți, 284
 servere intermediar interne, 146-147
 Service, pagină de proprietăți, 281
 servicii Internet, 286-287
 serviciul Web Proxy, 279
 tn-gw (comenză), 233
Proxy Settings, casetă de dialog, 146, 256, 286-287
ps, comandă, 119, 157
PTR, tip de înregistrare, 53-54
 publicare în Web, 284
 Publishing, pagină de proprietăți, 284-285
 punct (.), 49
 puncte finale, 46

Q-R

quit, comandă, 233
-r port, opțiune în linia de comandă, 262
-R regulă de înlănțuire-regulă de număr, comandă, 268
-R, parametru în linia de comandă, 254
r*, instrumente (program de corectare ssh), 371
r, servicii (UNIX), 115
r, utilitare, 55-56
 radio, butoane
 Audit These Events, 158
 Do Not Audit, 159
 Event Log Wrapping, 163
 Log to File, 285
 Log to SQL(ODBC, 285
 Manual Proxy Configuration, 256
rapoarte, 303
RAS (server de acces de la distanță), 176-177
rcp, utilitar, 56
 reconfigurarea informațiilor despre gazde/rețea (atacuri prin blocarea unui serviciu), 63
Red Hat, sit Web, 259
 Redirect Message, tip de mesaje, 34
 Redirect, tip de mesaje, 65-66
 redirecționarea țintei, 266

refacerea regulilor, 270-271
Refresh Rate, câmp, 54
Regular, format de înregistrare în jurnal, 285
reguli, *vezi și* înlănțuirii
 creare, 225-226
 cuvinte cheie, 225
 gestionare, 268-269
 ipfwadm, 259-260, 264
 liste de valori pentru atribute, 225
 restaurare, 270-271
 rutere, 108-109
 salvare, 270-271
 specificarea parametrilor, 268
 ștergere, 268
reject, cuvânt cheie, 266
reject, politică, 261
reject, țintă, 266
Remote Login, intermediar, 233
Remote Monitoring (RMON), 58
Replace Auditing on Existing Files, casetă de validare, 160-161
Replace Auditing on Subdirectories, casetă de validare, 160-161
 repornirea demonului inetd, 212, 223
Request for Comments, documente. *vezi* documente
RFC
Restart, comandă (CommandView Firewall), 296
Restart, Shutdown and System, eveniment, 159
 restricționarea accesului la Internet, 15
 resurse (limitate), supraîncărcare (atacuri prin blocarea unui serviciu), 63
 resurse limitate, supraîncărcare (atacuri prin blocarea unui serviciu)
 resurse suplimentare, 372
 CERT Coordination Center, 373-374
 COAST (Computer Operations, Audit and Security), sit Web, 376
 Federal Computer Incidence Response Capability, sit Web, 376
 Forum of Incident Response and Security Teams, 372
 Lopht Heavy Industries, sit Web, 375
 liste poștale pentru firewall-uri, 375
 Microsoft, situri Web, 374
 National Security Institute's Security Resource Net, sit Web, 376-377

SANS (System Administration, Networking and Security)
 Institute, 373
 securitate în NT, 375
 Security Portal, sit Web, 374
 situri Microsoft, 374
 U.S. Department of Energy, sit Web, 376
 World Wide Web Security FAQ, sit Web, 375
retransmiterea traficului (UDP), 246-247
Retrieve Plan from Firewall, comandă (meniul Command View File), 294
Retry Rate, câmp, 54
return, cuvânt cheie, 266
return, țintă, 266
rețea, strat OSI, 29
rețele
 fișiere gazdă, 139
 informații DNS, 138-139
 politici de securitate, creare, 17-19
 private (adrese), 39
 rețele de mare suprafață (WAN), 58, 61
 rețele locale. *Vezi* LAN
 rețele rivale, adrese, 39
 revizuire
 fișier de configurare syslog, 154-155
 fișiere jurnal, 148-151, 162-163
 plăci de rețea, 290
rexec, utilitar, 56
 rezervat, câmp, 183
 rezumatul mesajelor, 170
 .rhosts, fișier, 56, 233
 rlogin, intermediar, 233
 rlogin, utilitar, 56
 rlogin-gw, poartă intermediar, 233-234
RMON (Remote Monitoring), 58
 root, domeniu, 50
 rotația fișierelor jurnal SQUID, 255
 Routing, pagină de proprietăți, 284
rpcbind, program demon, 117
RSA, criptare cu chei publice, 188
rsh, utilitar, 56
rutare
 program de configurare (CommandView Firewall), 290-293
 software de intermediere pe gazde bastion, 129-130
 /rules, director (subdirectoare), 205-206
 ruptime, utilitar, 56
 rutare, 134, 258

rutare la sursă, 62
 definire, 45
 dezavantaje, 62
 slabă, 45
 strictă, 45
rutare slabă la sursă, 45
rutare strictă la sursă, 45
rutere, 34, 81-82
 filtrarea pachetelor, 32, 109
 liste pentru controlul accesului (reguli), 108-109
 rutere cu ecranare, 81-82, 95
rutere cu ecranare, 81-82, 95
rutere cu filtrarea pachetelor, 109
rutere cu filtrarea pachetelor, configurare, 32
rwho, comandă, 155-156
rwho, utilitar, 56

S

%s, variabilă, 214
-S adresă [mască] [port ...], parametru, 262
-s sursă, parametru, 268
-s tcp tcpfin udp, comandă, 261
-s, parametru în linia de comandă, 254
SA (Security Association), durată de valabilitate, 181
SA, adresă sursă, 181
SA, criptare, 188
SA, criptare cu chei publice, 188
 salvarea regulilor, 270-271
SAM (Security Account Manager), bază de date, 59-60
SANS (System Administration, Networking and Security)
 Institute, 373
SANS (System Administration, Networking and Security)
 Institute, sit Web, 373
SAPs (Service Access Points), 28-29
SATAN (Security Administrator Tool for Analyzing Networks), 366-367
SATAN (Security Administrator Tool for Analyzing Networks), sit Web, 205-206, 366-367
Save Plan to File, comandă (meniul Command View File), 294
Save Plan to Firewall, comandă (meniul Command View File), 294
 scanare împotriva virusilor, 306
 schimbarea cheilor, 168, 181
 scriere aleatorie, prompt, 190-191
 script (configurare), 252
 script de configurare, 252

Search, buton, 161
Secure Shell, 116
Secure Sockets Layer (SSL), 300
Secure Sockets Layer (SSL), protocol, 169, 172-173, 175
Secure Sun, 368
Secure Sun, sit Web, 368
SecureID, 114
securitate, 10. *Vezi și* firewall-uri
 anteturii de pachete, 13-14
 atacuri prin blocarea unui serviciu, 63
 avantajele firewall-urilor, 23
 calculatoare casnice, 308-309
 Destination Unreachable, tip de mesaje, 66
 educarea utilizatorilor, 72
 filtre de pachete, 13-14, 19-20
 instrumente de verificare a securității sistemului, 368-369
 intermediere de aplicații, 19-20
 Internet, 16-17
 IPSec, suită de protocoale, 179-180
 limitele firewall-urilor, 23-24
 parole (utilitare pentru parole), 364-367
 pătrunderi în sistem, 71
 prevenirea inundațiilor SYN, 64-65
 protocoale de rețea, 61-62
 protocoale IP (rutare la sursă), 62
 Redirect, tipuri de mesaje, 65-66
 rețea (dispozitive firewall), 302
 rețele locale, 58
 autentificarea utilizatorilor, 59-60
 măsurile fizice de siguranță, 61
 protejarea resurselor, 60-61
 TCP/IP, 61-62
 WANS, 61
securitatea calculatoarelor casnice, 235-236
securitatea parolelor (utilitare pentru parole), 364-367
securitatea rețelei (dispozitive firewall), 302
Security Accounts Manager (SAM), bază de date, 59-60
Security Administrator Tool for Analyzing Networks (SATAN), 205-206, 366-367
Security Parameter Index (SPI), 181
Security Parameter Index (SPI), câmp, 183
Security Policy Changes, eveniment, 159
Security Portal, sit Web, 374
Security, buton, 278
Security, casetă de dialog, 286

Security, comandă (meniul Log), 163
Security, etichetă, 160-161
Security, fișier jurnal pentru evenimente, 162-163
Select Components, casetă de dialog, 193
Select Program Folder, casetă de dialog, 291
Select User Service for Master Security Plan, casetă de dialog, 297
selectare
 componente PGP, 192-193
 dispozitive firewall, 305
 firewall-uri, 21-22
selectoare, 152-153
semn de exclamare (!), 232
semnături digitale, 70, 169-170, 192
semnături digitale, creare, 192
semnul exclamării în cerc galben, 163
Send SMTP Mail, casetă de validare, 286
sendmail, 234, 369
sendmail program, comandă, 236
sendmail, program demon, 210
separarea acțiunilor și selectoarelor, 154
Sequence Number, câmp, 64, 183
Serial Number, câmp, 54
Server Backup, buton, 281
server de acces de la distanță (RAS), 176-177
server de căutare DNS, 203
server intermediar personalizate, creare, 139
Server Restore, buton, 281
Server, câmp, 211, 222
servere
 cache, 203
 copii, 255
 părinte, 255
 rude, 255
 SQUID, 253
 căutare DNS, 203
 cheie, 190-191
 comunicații între servere părinte și copii (SQUID), 203
 copii, 203
 DNS, 52
 fișiere, 52
 numai pentru cache, 51
 principal, 51
 secundar, 51
 inetd, server demon, 116
 intermediar, 83-84, 132-135, 27, 217-218, 245
 intermediar cu cache, 249
 acces transparent la serviciile de rețea, 146-147

- avantaje/dezavantaje, 135
 blocarea accesului la Internet, 144-145
 blocarea traficului IP, 132-133, 137
 configurare, 227
 dezactivarea rutării, 134
 ecranarea accesului la Internet, 144-145
 intermediare proprii, creare, 139
 înregistrare în jurnal, 145
 servere intermediar interne, 146-147
 în-gw (comenzi), 233
 părinte, 203
 păstrare în cache, 11, 247-248.
 Vezi și SQUID
 SOCKS, 201
 alocarea soclurilor, 242-243
 configurații, 242-243
 descărcare, 247-248
 stabilirea conexiunilor client/server, 242-244
 SQUID, 203, 251
 Telnet, 47
 servere copil, 203
 servere de cache, 14, 202, 203
 copil, 255
 părinte, 255
 rude, 255
 SQUID, 253
 servere de cache copil, 255
 servere de cache rude, 255
 servere de chei, 190-191
 servere DNS
 fișiere, 52
 numai de cache, 51
 principale, 51
 secundare, 51
 servere independente (Windows NT Server), 160-161
 servere intermediar cu cache, 248, 302. Vezi și SQUID
 servere intermediar interne, 146-147
 servere intermediar transparente, 137-138
 servere numai de cache (DNS), 51
 servere primare (DNS), 51
 servere secundare (DNS), 51
 Service (Windows NT), casetă de dialog, 119
 Service Properties, comandă (meniul Properties), 277
 Service, etichetă, 286
 Service, pagină de proprietăți, 281
 /services, subdirector (directorul /rules), 205-206
- Services Access Points (SAP), 28-29
 Services, miniaplicație (Windows NT), 119
 servicii FTP (UNIX), 115
 servicii pentru utilizatori, gestionare, 297
 servicii Windows NT, 119-120
 sesiune, strat OSI, 29
 Set Date/Time, comandă (CommandView Firewall), 295
 Set Group ID (SGID), 122-123
 Set Notification Command, casetă de dialog, 292-293
 Set Password, comandă (CommandView Firewall), 295
 Set User ID (SUID), 122-123
 Settings, comandă (meniul Command View File), 163
 Settings, comandă (meniul File), 163
 Setup Complete, casetă de dialog, 291
 Setup Type, casetă de dialog, 290
 SGID (Set Group ID), 122-123
 shareware, 198
 Show Users, buton, 161, 281
 simbol diez/ simbol pentru numere (#), 154, 225
 simbol pentru numere/simbol diez (#), 154, 225
 Simple Mail Transfer Protocol (SMTP), 18, 55, 70
 Simple Network Management Protocol (SNMP), 58, 304
 Simple WATCHer (SWATCH), 366
 sincronizarea fișierelor de parole, 59-60
 sisteme de operare
 alegerea firewall-urilor, 21-22
 sisteme de operare sigure, instalare pornind de la zero, 114
 sisteme de operare sigure, instalare pornind de la zero, 114
 situri FTP (anonime), 18, 48
 Skey, 114
 Slipjack, 168
 smap, 201, 220, 234
 cuvinte cheie, 235
 lansare, 236
 smapd, 201, 220, 234
 cuvinte cheie, 235-236
 lansare, 236
 smrsh, 369
 smrsh, sit Web, 369
 SMTP (Simple Mail Transfer Protocol), 18, 55, 70
 SMXP Encryption Key, comandă (meniul CommandView Firewall), 296
- SNMP (Simple Network Management Protocol), 58, 304
 SOA (Start of Authority), înregistrare, 52
 SOA, câmp, 53
 SOA, înregistrare, 53-54
 SOA, tip de înregistrare, 53
 SOCK-et-S. Vezi SOCKS
 SOCKS (SOCK-et-S), 84, 201-202, 242
 asistență tehnică, 247-248
 legarea codului de funcțiile de bibliotecă, 247
 liste poștale, abonare, 247-248
 SOCKS Command Code, valori pentru câmp, 242-243
 SOCKS V4, 241
 cereri BIND, 244
 cereri CONNECT, 242
 SOCKS V5, 245-246
 SOCKS V5 Command Code, valori pentru câmp, 242-243
 SOCKS V5 Reference Implementation, descărcare, 247-248
 SOCKS, server, 201
 alocarea soclurilor, 242-243
 configurații, 242-243
 descărcare, 247-248
 stabilirea conexiunilor client/server, 242-244
 SOCKS, sit Web, 241
 SocksCap, 241, 247
 „SOCKSificarea” aplicațiilor, 202, 247
 socluri
 /dev/log, 152
 alocare, 242-243
 filtre de pachete, 103-104
 software (intermediar), rulare pe gazde bastion, 129-130
 software de criptare, PGP (Pretty Good Privacy). Vezi PGP
 software de intermediere, rulare pe gazde bastion, 129-130
 Source Address, câmp, 44, 73, 312-313
 Source Quench, tip de mesaje, 34
 spargerea parolelor, 71
 spațiu de adrese (LAN), creștere prin NAT, 142-143
 Special Directory Access (Windows NT), casetă de dialog, 128
 specificare
 acțiuni, 154
 adrese, 269
 adrese IP, 268-269
 dimensiunea cheii, 190
 domenii de adrese, 269
 domenii de porturi, 269

- măști de rețea, 269
 numere de porturi, 268-269
 reguli (parametri), 269
 SPI (Security Parameters Index), 181
 SPI (Security Parameters Index), câmp, 183
 SQUID, 202-203, 249-250
 comunicații între servere părinte și copil, 203
 configurarea clienților, 256
 descărcare, 250
 fișiere jurnal, 254-255
 gestionare, 252
 ierarhie de cache, 255
 instalare, 250-252
 servere, 203
 alegere, 251
 căutare DNS, 203
 de cache, 203
 squid, comandă, 252-255
 squid, crearea conturilor de utilizator, 250
 squid, parametri în linia de comandă, 253-254
 -a port, 253
 -D, 254
 -d nivel de eroare, 253
 -f, 253-254
 -h, 253
 -k, 253
 -k check, 253
 -k debug, 253
 -k interrupt, 253
 -k kill, 253
 -k rotate, 253
 -k shutdown, 253
 -N, 254
 -R, 254
 -s, 254
 -u, 254
 -v, 254
 -X, 254
 -Y, 254
 -z, 254
 SQUID, server de cache, 253
 SQUID, sit Web, 250, 253
 squid.conf, fișier, 203, 252-253
 SRA, 370
 SRA, sit Web, 370
 ssh, 371
 SSH Secure Shell, sit Web, 116
 ssh, sit Web, 371
 SSL (Secure Sockets Layer), 300
 SSL (Secure Sockets Layer), protocol, 169, 172-173, 175
 SSL (Secure Sockets Layer), protocol de confirmare, 172-173
 SSL (Secure Sockets Layer), protocol de înregistrare, 172
- stabilirea conexiunilor client/server (server SOCKS), 242-244
 Stacheldraht, 67
 Start of Authority, înregistrare, 52
 stive de protocoale, 26-27
 stocarea cheilor, 190-191
 store.log, fișier, 254
 strategii (firewall-uri), 81-87, 89-92
 arhitectură de subrețea ecranată, 88-90
 combinarea strategiilor, 85-88
 gazde cu două plăci de rețea, 86-87
 gazde ecranate, 87-88
 filtre de pachete, 81-83
 gazde bastion, 89-92
 gazde de sacrificiu, 89-92
 porți pentru intermedierea aplicațiilor, 83-84
 straturi, 28
 aplicație, 27, 30
 controlul accesului la mediu (MAC)
 controlul legăturii logice (LLC), 28-29
 fizic, 28
 legătură de date, 28-29
 prezentare, 27, 30
 rețea, 29
 sesiune, 29
 transport, 29
 su (program fals), sit Web, 371
 su, comandă, 156
 su, program fals, 371
 subdirectoarea (directorul /rules), 205-206
 subdomenii, 51
 subrețele, 40
 subrețele ecranate, 97
 subrețele ecranate multiple, 89-92
 succes, înregistrarea în jurnal a evenimentelor, 158
 Success, casetă de validare, 158
 SUID (Set User ID), 122-123
 suite de protocoale, 26-27, 179-180
 supraîncărcarea resurselor limitate (atac prin blocarea unui serviciu), 63
 swap.state, fișier, 255
 SWATCH (Simple WATCHer), 366
 SWATCH (Simple WATCHer), sit Web, 366
 SYN Flag, câmp, 64
 SYN, bit, 105-106
 SYN, inundare, 64-65, 105-106
 syslog, fișier de configurare
 modificarea valorilor prestabilite, 152
 niveluri de severitate, 152-153
 nume de utilitare, 152-153
 revizuire, 154-155
 transmiterea mesajelor către alte calculatoare, 154-155
 syslog, program demon (syslogd), 151-152, 200-201, 210, 220, 239
 syslog, utilitar, 151-152
 syslogd (demon syslog), 151-152, 200-201, 210, 220, 239
 syslogd.conf, fișier, 210
 System Administration, Networking and Security (SANS) Institute, 373
 System, fișier jurnal pentru evenimente, 161
- S**
- ștergere
 chei publice din inelele de chei, 191
 fișiere jurnal, 150
 reguli, 268
- T**
- t andmask ormask, opțiune în linia de comandă, 270
 -t andmask xormask, opțiune în linia de comandă, 243
 tabele (ARP), 33
 talkd, demon, 116
 TCP (Transmission Control Protocol), protocol, 32, 208, 318
 TCP Protocol Data Unit, 101
 TCP Wrappers, 116, 199-201, 208-209
 configurare, 210-211
 fișierul hosts.allow, 212-215
 fișierul hosts.deny, 212-215
 fișierul inetd.conf, 211-212
 controlul accesului, 199, 208-209
 descărcare, 200
 înregistrare în jurnal, 200, 209-210
 limite, 215
 obținere, 210
 tcpd, demon, 199, 209
 TCP, numere de porturi recunoscute, 318-363
 TCP, protocol (metodă de conectare cu confirmare în trei etape), 64
 TCP/IP (Transmission Control Protocol/Internet Protocol), 26-27, 30-32, 47, 57, 208
 probleme de securitate, 61-62
 Telnet, 47

tcpd (TCP Wrappers), program demon, 199, 209, 211
 tcpdchk, 215
 tcpdmatch, 215
 tcpdump, 368
 tcpdump, sit Web, 368
 Telnet, 18, 47, 116, 208, 370
 Telnet, server intermediar, 231
 Telnet, servere, 47
 telnetd, 201, 220
 testarea firewall-urilor, 308
 text cifrat, 166
 TFN (Tribe Flood Network), 67
 TFN2K (Tribe Flood Network 2000), 67
 TFTP (Trivial File Transfer Protocol), 49, 109
 Tiger, 365
 Tiger, listă poștală, 366
 Tiger, sit Web, 365
 Time Exceeded, tip de mesaje, 14
 Time to Live (TTL), câmp, 44
 timeout secunde, comandă, 233, 235-237
 Timeout secunde, cuvânt cheie, 227-229
 Timestamp Reply, tip de mesaje, 34
 Timestamp Request, tip de mesaje, 34
 tipuri (ICMP), 264-265
 tipuri de înregistrări, 53-55
 tipuri de înregistrări DNS, 53-55
 tipuri de mesaje
 Address Mask Reply, 34
 Address Mask Request, 34
 destination Unreachable, 34, 66
 Echo Reply, 34, 65
 Echo Request, 34, 65
 ICMP, 34
 Information Reply, 34-35
 Information Request, 34-35
 Parameter Problem, 34
 Redirect, 65-66
 Redirect Message, 34
 Source Quench, 34
 Time Exceeded, 34
 Timestamp Reply, 34
 Timestamp Request, 34
 TIS (Trusted Information Systems), 217-218
 TIS (Trusted Information Systems) Firewall Toolkit. *Vezi* FWTK
 TLS (Transfer Layer Security), protocol, 173-174
 tn-gw, 220
 tn-gw proxy, cuvinte cheie, 232
 tn-gw, comenzi pentru server intermediar, 233
 tn-gw, intermediar, 231

/todo, subdirector (/directorul /rules), 205-206
 Toolkit. *Vezi* FWTK
 Tools, meniu (Internet Options), 256
 touch (UNIX), comandă, 135
 TRACEROUTE, comandă, 34
 Traffic Class, câmp, 312
 trafic (UDP), retransmitere, 246-247
 trafic de rețea, monitorizare, 72-73
 Transfer Layer Security (TLS), protocol, 173-174
 transferare
 fișiere între calculatoare, 48
 pachete, 31-32
 transferuri pe zone, 51
 translatare, adrese hardware/IP
 translatarea adreselor, 14
 Transmission Control Protocol (TCP), 32, 208, 318
 Transmission Control Protocol/Internet Protocol. *Vezi* TCP/IP
 transmiterea datelor (tuneluri PPTP), 186
 transmiterea mesajelor către alte calculatoare (fișier de configurare syslog), 154-155
 transport, strat OSI, 29
 Tribe Flood Network (TFN), 67
 Tribe Flood Network 2000 (TFN2K), 67
 Trin00, 67
 Trip Wire, sit Web, 369
 Tripwire, 92, 369
 Tripwire Security Systems, sit Web, 92
 Trivial File Transfer Protocol (TFTP), 49, 109
 trojan.pl, 368
 trojan.pl, sit Web, 368
 /trust, subdirector (directorul /rules), 205-206
 Trusted Information Systems (TIS), 217-218
 Trusted Information Systems Firewall Toolkit. *Vezi* FWTK
 tuneluri (PPTP), 212, 222-224.
Vezi și VPN
 TXT, tip de înregistrări, 53
 Type of Service (TOS), câmp, 43

T

ține
 accept, 266
 accept, 266
 deny, 266
 masq, 266

redirect, 266
 reject, 266
 return, 266

U

%u, variabilă, 214
 -u, parametru în linia de comandă, 254
 -user userid, cuvânt cheie, 227
 U.S. Department of Energy, sit Web, 376
 UDP (User Datagram Protocol), 26-27, 32, 208, 318
 UDP ASSOCIATE, cereri (SOCKS V5 Command Code), câmp, 246
 UDP ASSOCIATE, pachet de cerere, 246
 UDP, antet de cerere, 246
 UDP, fragmentare, 246
 UDP, informații de antet (filtre de pachete), 103-104
 UDP, intermediar, creare, 245-246
 UDP, numere de porturi recunoscute, 318-363
 UDP, port 514, 152
 UDP, porturi, 46
 UDP, trafic, retransmitere, 246-247
 UID (identificator de utilizator), 211
 UID, câmp, 211, 221
 UNIX, 151
 auditare (utilitar syslog), 151-152
 automatizarea operațiilor, 156
 comenzi, înlocuire/corectare, 369
 dezactivarea rutării pe serverele intermediar, 134
 fișier ascuns de parole, 114
 fișiere de configurare în rețea, 118
 fișiere jurnal, 155
 /etc/utmp, 155-156
 /usr/adm/wtmp, 155-156
 /var/adm/aculog, 156
 /var/log/cron, 156
 lastlog, 155-156
 instalarea PGP, 189
 compilarea codului sursă, 189
 generarea perechilor de chei publică/secretă, 189-190
 stocarea cheilor, 190-191
 permisiuni de acces la resurse, 121-124
 SGID (Set Group ID), 122-123
 SUID (Set User ID), 122-123
 valori pentru permisiuni, modificare, 123-124
 valori pentru permisiuni, vizualizare, 122

valori pentru proprietar, modificare, 123-124
 procese demon, 115-116
 inetd.conf, fișier de configurare, 115-116
 NFS (Network File System), 117
 syslogd, demon, 210
 touch, comandă, 135
 Unix to Unix Copy Program (uucp), 116
 UNIX, variabile de mediu, definire, 189
 UNKNOWN, cuvânt cheie, 213
 Upgrade, comandă (CommandView Firewall), 296
 URL, 284
 URL, blocare, 144
 /usr/adm/wtmp, fișier, 155-156
 /usr/local/etc/netperm-table, 225
 Use of User Rights, eveniment, 159
 User and Group Management, eveniment, 159
 User Datagram Protocol. *Vezi* UDP
 User ID, câmp (CONNECT Request), 242-243
 User Manager, 158-161
 User Manager, comandă (meniul Administrative Tools), 158
 userID (UID), 211
 userid utilizator, comandă, 235-237
 userid utilizator, cuvânt cheie, 229
 utilitare
 PGP (Pretty Good Privacy), 188
 accesul la fișiere criptate, 192
 configurare, 194-195
 crearea semnăturilor digitale, 192
 instalare, 189-190, 192-193
 r, 55-56
 syslog, 151-152
 utilizatori, baze de date centralizate, 60
 utilizatori, educarea privind securitatea, 72
 uucp (Unix to Unix Copy Program), 116

V

-V adresă, parametru, 262
 -v, opțiune, 270-271
 -v, opțiune în linia de comandă, 263, 270
 -V, parametru în linia de comandă, 254

validitate SA (asocieri de securitate), 181
 valori
 calcularea subrețelelor, 41
 politică, 261
 potrivirea atributelor, 225-226
 valori de proprietar (proprietăți UNIX pentru resurse), 123-124
 valori pentru politici, 261
 valori pentru proprietăți (permisiuni pentru resurse UNIX)
 modificare, 123-124
 vizualizare, 122
 valori pentru subrețea, calculare, 41
 valorile atributelor, potrivire, 226, 229, 232
 /var/adm/aculog, fișier, 156
 /var/log/cron, fișier, 156
 variabile
 %, 214
 %a, 214
 %c, 214
 %d, 214
 %h, 214
 %n, 214
 %p, 214
 %s, 214
 %u, 214
 comenzi de nucleu, 214
 de mediu, definire, 189
 variabile de mediu, definire, 189
 vectorizarea adreselor, 15, 143
 Verbose, format de înregistrare în jurnal, 285
 verbose, indicator, 270
 verificarea paginilor Web pentru criptare, 173-174
 Verisign, sit Web, 172
 Version Number, câmp, 246
 cerere CONNECT, 241
 cod de răspuns, 242-243
 Version, câmp, 43, 312
 versiune de probă (CommandView Firewall), descărcare, 287
 View, buton, 256
 View, comenzi de meniu (Internet Options), 286-287
 View, meniu (CommandView Firewall), 294
 Virtual Private Network Consortium (VPNC), 176
 Virtual Private Networks. *Vezi* VPN
 viruși, 24, 68-70, 145
 vizualizarea conținutului inelelor de chei, 191
 VPN (rețele virtuale private), 60, 73, 176, 188, 300, 304, 309
 autentificare, 176-177

avantaje, 177-178
 creare, 176-177
 dezavantaje, 178-179
 intrare în rețea, 176
 VPNC (Virtual Private Network Consortium), 176

W

-W nume, parametru, 262
 Wait-state, câmp, 211, 221
 wakeup secunde, comandă, 236
 WAN (rețele de mare suprafață), 58, 61
 Web Proxy, serviciu, 279
 AutoDial, 280
 componente de completare produse de alte firme, 280-281
 intrarea într-o matrice de servere proxy, 280-281
 Web, situri
 „Improving the Security of your Site by Breaking Into It” (Dan Farmer & Wietse Venema), 205-206
 altavista, 372
 Argus, 366
 Authd, 370
 Blowfish, 371
 Caldera, 258
 CERT Coordination Center, 373-374
 COAST (Computer Operations, Audit and Security), 376
 Computer Incident Advisory Capability, 67
 COPS (Computer Oracle and Password System), 365
 Courtney, 367
 Crack, 365
 Drawbridge, 204
 Federal Computer Incidence Response Capability, 376
 fingerd, 370
 Firewalls, listă poștală, 375
 Forum of Incident Response and Security Teams, 372
 Free Software Foundation, 249
 FreeBSD, 204
 FWTK, 217-218, 239
 Gabriel, 367
 IETF, 173-174
 ifstatus, 367
 ipchains, 264-265, 271
 ipfwadm, 259
 IPv6, 309-310
 ISS (Internet Security Scanner), 366
 L0pht Heavy Industries, 375
 Isot, 369
 MD5, 369

Merlin, 368
 Microsoft, 114, 374
descărcarea pachetelor de servicii, 273
securitate, 374
 National Security Institute's Security Resource Net, 376-377
 Network Associates, 188
 NID (Network Intrusion Detector), 368
 NT, securitate, 375
 PCERT, 373-374
 Perl COPS (Computer Oracle and Password System), 365
 PortMap V3, 370
 Red hat, 258
 SANS (System Administration, Networking and Security) Institute, 373
 SATAN (Security Administrator Tool for Analyzing Networks), 205-206, 366-367
 Secure Sun, 368
 Security Portal, 374
 sfingerd, 370
 smrsh, 369
 SOCKS, 241
 SQUID, 250, 253
 SRA, 370
 ssh, 371
 SSH Secure Shell, 116
 su (program fals), 371
 SWATCH (Simple WATCHer), 366
 tcpdump, 368
 Tiger, 365
 Trip Wire, 369
 Tripwire Security Systems, 92
 trojan.pl, 368
 U.S. Department of Energy, 376
 Verisign, 172
 World Wide Web Security FAQ, sit Web, 375

welcome-msg nume_de_fişier, cuvânt cheie, 229
who, comandă, 155-156
Windows NT
 Add Users and Groups, casetă de dialog, 127
 auditare, 157-158
configurarea evenimentelor pentru auditare. Vezi evenimente, auditare
dezactivarea auditării, 159
Event Viewer, 157
 configurare PGP, 194-195
 dezactivarea rutării pe serverele intermediar, 134
 Directory Permissions, casetă de dialog, 127-129
 Explorer
modificarea permisiunilor, 127-128
vizualizarea permisiunilor pentru fişiere/directoare, 126-127
 fişiere jurnal
gestionare, 163
revizuire, 162-163
 imprimante, auditarea utilizării, 161
 instalare PGP, 192-193
 Network, miniaplicație, 119
 permisiuni pentru resurse, 125-129
modificare, 127-129
permisiuni speciale, 125
permisiuni standard, 125-126
vizualizarea permisiunilor pentru fişiere/directoare, 126-127
 Service, casetă de dialog, 119
 Services, miniaplicație, 119
 servicii, 119-120

Special Directory Access, casetă de dialog, 128
 Windows NT Explorer, 158-161
 Windows NT Explorer, comandă (meniul Programs), 160-161
 Windows NT Server, 160-161
 Windows NT Service Packs, 114, 273
 WinSock, funcții de rețea, interceptarea apelurilor, 241, 247
 wizard, generarea cheilor, 194, 196
 WKS, tip de înregistrare, 53
 World Wide Web Security FAQ, sit Web, 375
 WWW (World Wide Web), 18
 X Windows, 100
 x-gw, comandă, 233

X-Z

-X înlănțuire, comandă, 267
-x, opțiune în linia de comandă, 263, 270
-X, parametru în linia de comandă, 254
-y, opțiune în linia de comandă, 263, 270
-Y, parametru în linia de comandă, 254
-Z înlănțuire, comandă, 268
-z, comandă, 261
-z, parametru în linia de comandă, 254
 Xforwarder program, cuvânt cheie, 232
 Yellow Pages, 59-60
 Zimmerman, Phillip (PGP), 188
 Zis, 51
 zonă demilitarizată. *Vezi DMZ*
 zone virtuale de securitate, 302